PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : G06F 13/00

A1

(11) International Publication Number: **WO 00/46681**

(43) International Publication Date: 10 August 2000 (10.08.00)

(21) International Application Number: PCT/US00/03489

(22) International Filing Date: 8 February 2000 (08.02.00)

(30) Priority Data:

09/248,370	8 February 1999 (08.02.99)	US
60/153,901	14 September 1999 (14.09.99)	US

(63) Related by Continuation (CON) or Continuation-in-Part (CIP) to Earlier Applications

US	09/248,370 (CIP)
Filed on	8 February 1999 (08.02.99)
US	60/153,901 (CIP)
Filed on	14 September 1999 (14.09.99)

(71) Applicant *(for all designated States except US)*: GEOTRUST, INC. [US/US]; Suite 20, 40 Washington Street, Wellesley Hills, MA 02481 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: COULTHARD, Christopher, M. [GB/US]; 88 Park Avenue #402, Arlington, MA 02476 (US). MCLEOD, Scott, C. [US/US]; 24 Carriage Drive, Chelmsford, MA 01824 (US). NORMAN, Peter, D. [US/US]; 56 Palmer Street, Arlington, MA 02174 (US). WILLOUGHBY, Kevin [US/US]; 10 Church Street, Framingham, MA 01702 (US). HODGMAN, Rod, G. [US/US]; 465 Robinson Road, Boxborough, MA 01719 (US). ROSENBERG, Jonathan [–/US]; 11 Seton Hill Road, Auburndale, MA 02466 (US).

(74) Agents: LEE, G., Roger et al.; Fish & Richardson P.C., 225 Franklin Street, Boston, MA 02110–2804 (US).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published

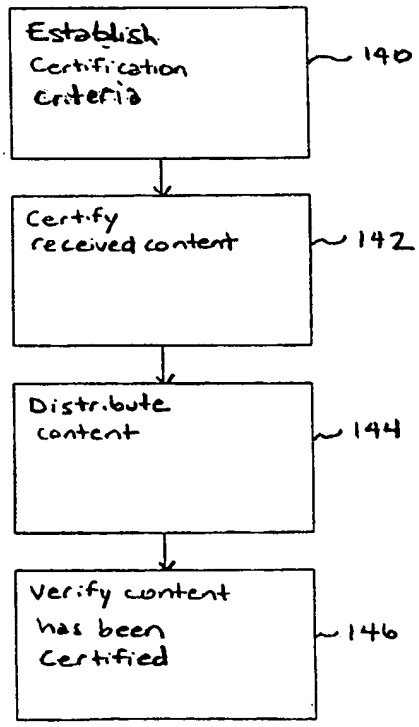
With international search report.

Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: CONTENT CERTIFICATION

(57) Abstract

A method of processing content includes storing verification information corresponding to certified content at a first computer (140) and receiving a verification request corresponding to content from a second computer (142). The method also includes determining a verification information for the content corresponding to the verification request and comparing the determined verification information with the stored verification information (146).



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

CONTENT CERTIFICATION

Reference to Related Applications

This application relates to pending U.S. application Serial No. 09/248,370, entitled "Content Certification", filed on February 8, 1999 and U.S. Provisional Application Number 60/153,901 filed September 14, 1999. These applications are incorporated by reference in their entirety herein.

Background of the Invention

The Internet and the World Wide Web have made information dissemination fast, easy, and cheap. Postings from both businesses and individuals have contributed to the wealth of available information. Unfortunately, the available information is sometimes of dubious value. For example, in 1998 a news agency accidentally posted a pre-written obituary of Bob Hope on its Web-site. Congress held a moment of silence in his honor. The report of Mr. Hope's demise, however, was greatly exaggerated. Other Internet postings have been less innocuous such as the accidental pre-release of economic data by the U.S. Bureau of Labor and Statistics.

In addition to accidental postings, some information available on the Internet, purporting to be from official sources, includes intentionally fabricated data or malicious statements. As a result, users tend to be somewhat skeptical of information accessed from the Internet. Additionally, some businesses, wary of potential liability or embarrassment, have begun to err on the side of safety and withhold information from Internet publication. These factors combine to reduce the effectiveness of the Internet as a communication medium.

Summary of the Invention

In general, in one aspect, a method of processing content includes storing verification information corresponding to certified content at a first computer and

receiving a verification request corresponding to content from a second computer. The method determines verification information for the content corresponding to the verification request and compares the determined verification information with the stored verification information.

Embodiments may include one or more of the following features. The method may feature receiving content certification criteria that can be used to determine whether content should be certified. The content certification criteria can be a list of required approval or programmed logic. The method may also feature storing certification information (e.g., a type of certification granted, entities approving certification, and when the content was certified). The verification information can include information derived from the content such as at least one hash key.

The verification request can include a URL. This can enable determination of verification information by collecting content from the URL included in the verification request.

The verification request can include content. This can enable determination of verification information by determining verification information for the content included in the verification request.

The verification request can include verification information. This can enable determination of verification information by merely using information included in the verification request.

Receiving a verification request may be produced by user interaction with a certification indicator, for example, a certification indicator included in the content.

The certification indicator can include a graphic image having associated instructions that produce a verification request. The method may further include transmitting certification information to the second computer.

The content may include graphics, text, animation, sound, and instructions. The content may form a web-page.

The comparing may include issuing verification requests to connected certification servers.

In general, in another aspect, a method includes presenting an indication that content is certified and receiving user input requesting certification verification of the content. The method further includes transmitting a certification verification request to a certification server and receiving information indicating whether the content has actually been certified.

Embodiments may include one or more of the following features. Presenting an indication may include presenting a user interface control. The method may further include displaying information included in the information received (e.g., content authorship, revision number, expiration date, and type of certification).

Transmitting a certification verification request may include transmitting verification information determined from the content such as one or more hash keys. Transmitting a certification verification request may include transmitting information included in the content.

Transmitting a certification verification may include transmitting a URL.

In general, in another aspect, a method of controlling content distribution includes receiving certification criteria for content to be distributed,

identifying content to be distributed, and determining whether the identified content satisfies the received certification criteria.

Embodiments may include one or more of the following features. Identifying content may include receiving a request for content at a server. Identifying content may include collecting content from a set of locations. Determining whether the content satisfies the certification criteria may include identifying at least one digital signature associated with the content and/or determining verification information (e.g., a hash key) for the content.

Advantages may include one or more of the following features. The techniques provide users with a simple and intuitive method of verifying that content (e.g., a web-page) has been certified by an organization. Verification can be a mouse-click away when content includes a certification indicator. Underlying mechanisms protect the verification process from falsification and tampering. These mechanisms enable users to trust the authenticity of displayed content.

The techniques also enable an organization to carefully define certification procedures that content must undergo before certification and distribution. Automating these certification procedures enables an organization to vigilantly control the quality and reliability of information provided.

Different implementation architectures permit distribution of certification functions across different computers and potentially speeding certification verification.

Other advantages of the invention will become apparent in view of the following description, including the figures, and the claims.

Brief Description of the Drawings

FIG. 1 is a screenshot of content that includes a certification indicator.

FIG. 2 is a screenshot of information that verifies content certification.

FIG. 3 is a flowchart of a process for certifying content.

FIG. 4 is a flow diagram of a certification and certification verification of content.

FIG. 5 is a flowchart of a certification procedure.

FIG. 6 is a block diagram of a certification scheme.

FIGS. 7A and 7B are screenshots of user interfaces for submitting content for certification.

FIG. 8 is a flow diagram of content certification.

FIG. 9 is a flowchart of content certification.

FIG. 10 is a diagram of information stored at a certification server.

FIG. 11 is a diagram of digital signature blocks issued for certified content.

FIG. 12 is a block diagram of a certification server and certified content.

FIGS. 13-14 are flowcharts of processes for monitoring posted content.

FIGS. 15-16 are screenshots of graphical user interfaces that include certification indicators.

FIG. 17 is a diagram of a certification verification request.

FIGS. 18-22 are flowcharts of processes for certification verification.

FIG. 23 is a flowchart of a process for creating multiple certification servers.

FIG. 24 is a block diagram of a hierarchy of certification servers.

FIG. 25 is a flowchart of a certification verification process using multiple certification servers.

FIG. 26 is a block diagram of franchisee certification servers.

FIG. 27 is a flowchart of a process for transmitting content to a franchisee server.

FIG. 28 is a flowchart of a process for updating content offered by a franchisee server.

FIG. 29 is a screenshot of a browser's display of an Internet page.

FIGS. 30-36 are screenshots of different persistent displays that notify a user whether content is certified.

FIGS. 37, 39, 41, and 43 are diagrams of systems for validating content certification.

FIGS. 38, 40, and 44 are flow-charts of processes for validating content certification.

FIG. 42 is a diagram of a manifest of web-page contents.

FIG. 45 is a diagram of a certification server and a validation server.

Description of the Preferred Embodiments

Introduction

Referring to FIG. 1, a browser's graphical user interface 100 (e.g., Netscape™ Navigator™) presents content 104 provided by a resource (e.g., a file) at a URL (Universal Resource Locator) 102. The content 104 can include graphics, text, animation, sound, instructions (e.g., Java Applets), etc. A URL 102 can refer to a location on a remote computer that stores the content 104 as data and presentation instructions. The presentation instructions and data can be in a variety of formats such as HTML (HyperText Markup Language), XML (Extensible Markup Language), PDF (Portable Document Format), JPEG (Joint Photographic Experts Group), and MPEG (Moving Picture Experts Group). When a browser requests content 104 from a URL 102 resource, a remote computer providing the resource can transmit the content 104 to a browser for presentation. As shown, the browser is an independent application, however, other applications (e.g., an e-mail program, a word processor, or a spread-sheet) can incorporate functions traditionally performed by the browser.

As shown in FIG. 1, the browser display 100 includes a certification indicator 106. The indicator 106 provides a simple method of ensuring that the

content 104 presented has undergone a certification process. Content 104 may include one or more certification indicators 106 (e.g., "Certified by the Legal Department" and "Certified by the Marketing Department"). As shown, the indicator 106 is a user interface control that has a graphic image, however, different implementations can present the control to a user as text, sounds, or by using other user interface techniques. User selection of the indicator 106 (e.g., using a mouse or other pointing device to click on the graphic image) initiates a certification verification process that can confirm that the content presented is the same content that has undergone the certification process claimed by the certification indicator 106.

Referring to FIG. 2, the certification verification process can produce a window 108 that includes a display of information describing the content's 104 certification such as the entities that have approved the content 114, when such approval occurred 116, the version number 118, etc. Other user interface techniques can notify a user of certification. For example, a user interface can play voice data provided by a person who certified the data (e.g., "This web-page was approved by John Doe on February 8, 1999").

FIGS. 1 and 2 illustrate a simple and intuitive interface that ensures presented content is genuine. Underlying mechanisms protect the verification process from being falsified or mimicked. These mechanisms enable users to trust the authenticity of displayed content and provide web administrators with a tool for controlling content offered by a site.

Referring to FIG. 3, a certification process permits an entity (e.g., business, organization, or individual) to establish certification criteria 140. For example, a business can list employees that must approve submitted content 142 before it receives certification. After certification and distribution 144 of content (e.g., by posting the content on an Intranet, Extranet, or Internet site or e-mailing the content to recipients), mechanisms can verify 146 that the content presented to a user satisfies the criteria required for certification 140 and has not been

altered since certification. The process can then present certification information such as the entities that approved the content. Thus, users can view unforgeable information detailing the certification process undergone by content prior to distribution.

Referring to FIG. 4, an illustrative implementation uses a certification server 124 that includes instructions 126 for certifying submitted content 122. The certification instructions 126 can enforce certification criteria (e.g., all content must be approved by the legal department). The certification server 124 can include a database 128 for storing verification information determined from certified content. The verification information includes data that identifies the certified content such as a URL, compressed or uncompressed portions of the content, and/or an assigned identification number. The verification information may also include one or more hash keys (e.g., an MD5 hash and an SHA hash). A hash key is produced by a one-way function and typically requires little storage space (e.g., 160-bits). Hash keys are nearly guaranteed to be unique for any given content.

The database 128 can also store certification information such as the type of certification (e.g., the Legal Department), entities certifying the document, when certification occurred, when certification expires, the version of the certified content, etc. Certification information and verification information are not mutually exclusive categories. A piece of data may be both certification information and verification information.

As shown in FIG. 4, the certification server 124 also includes instructions 132 for processing requests 134 for certification verification. To verify certification, the instructions 132 can compare the verification information 130 stored during certification to verification information determined for the content being verified. A match indicates the content has undergone a certification process and has not been altered since. The certification server 124 can transmit information confirming certification of the content in question, for

example, by dynamically generating HTML instructions that includes certification information. An administrator can revoke certification by simply deleting or altering information in the database 128.

Defining a Certification Procedure

Referring to FIG. 5, an organization can use an interface to define different certifications 148 and criteria for granting the certifications 150 to submitted content. The criteria can include a simple list of employees that must approve submitted content. Criteria can also include programmed logic that tests for satisfaction of different conditions. The ability to program criteria enables a business to define certification processes that reflect a commitment to distributing thoroughly reviewed content.

Referring to FIG. 6, one possible certification scheme 152 uses different certification levels. As shown, the levels include site-wide certification 154, class certification 156-158, and individual certification 160-164. Each defined certification can include its own granting criteria. For example, to obtain site-wide certification, content must first receive certification from the Legal Department 156, the Marketing Department 158, and the company's CEO 164. Similarly, to receive Legal Department certification 156, at least two members of the legal department and a text-scanning program that looks for certain phrases must approve the content. As shown, the certification criteria can include different levels of abstraction. For example, instead of requiring certification from a particular named person, certification criteria can be more abstractly expressed, for example, as a role 162 (e.g., chief attorney) within an organization. This enables certification to continue as different persons fill positions.

The criteria for certification may include different levels of approval. For example, Marketing Department certification 158 may only require that each member of the marketing department receives content for review, while Legal Department certification may require that each member affirmatively indicates

approval of the content. Additionally, certification may be sought for internal (e.g., on an Intranet) or external publication (e.g., on the Internet). The criteria for external publication can be stricter than the criteria for internal publication.

The scheme 152 shown forms a hierarchy between the different certification levels 154-164. The hierarchical structure is a function of the defined criteria and is not an inherent characteristic of schemes having different certifications.

Content Certification

Referring to FIGS. 7A and 7B, easy-to-use graphical user interfaces shield users from the mechanics of submitting content for certification. For example, as shown in FIG. 7A, a user can submit content via a password protected web-page by dragging-and-dropping content onto one or more defined certification controls 156, 158. A control 156, 158 receiving the content can prepare and transmit a certification request indicating the content and the certification desired. The certification controls 156, 158 presented can vary depending on the person submitting content. Alternatively, as shown in FIG. 7B, an application toolbar 171 can include a "Certify" button 173. Selecting the button 173 can prepare and transmit a certification request for a document. The user interfaces of FIG. 7A and 7B are merely illustrative and other differently designed user interfaces could easily provide similar functions. Additionally, a system need not provide a graphical user interface at all, for example, by using e-mail to submit content for certification.

Referring to FIG. 8, a certification request 166 includes content 168 (or a reference to content) submitted for certification and other information 170 such as the certification desired (e.g., site-wide certification or Legal Department certification), the content authors, and a proposed URL. The request 166 can also include information such as a revision number, content keywords, title, etc. (not shown).

SSL (Secure Socket Layer), S-HTTP (Secure Hypertext Transfer Protocol), and other secure communications techniques can protect submitted content from tampering during transmission. Additionally, a request 166 can include one or more digital signatures (not shown) that enable a receiving computer to authenticate the source of the message. While these features enhance security and protect content from tampering en route to the certification server, the certification process does not require these measures.

The certification server 124 can process certification requests. The server 124 can distribute submitted content to individuals 172 that could potentially provide approval needed for certification. For example, the server 124 can distribute content to all the members of the Legal Department when a request is made for Legal Department certification. Workflow software, e-mail daemons, and other techniques, potentially executing on computers other than the certification server, can also distribute content to individuals for certification.

As shown in FIG. 8, after an entity 172 receives and reviews submitted content 168, the entity 172 can notify the certification server 124 of its approval by sending a certification message 174. The certification message 174 can include the submitted content 168 and other information 170 included in the certification request. The message can also include information 174 that describes the person transmitting the certification message 174a, the type of certification granted 174b (e.g., a person can have the capacity to certify content for both the marketing and the legal departments), and a level of approval 174c (e.g., "for internal use only" or "for publication on the Internet"). The certification message 174 may also include a digital signature 176 (e.g., a Verisign™/W3C X.509 digital certificate) belonging to the individual submitting the certification message 174 or may include information used by other authentication techniques such as biometric authentication. As shown in FIG. 8, the certification server 124 processes received certification messages 174 with certifying instructions 126.

Referring to FIG. 9, in one implementation, the certifying instructions 126 authenticate 178 a certification message to ensure the person claiming to have approved submitted content was, in fact, the person who produced the certification message 174. After authentication 178, the instructions 126 can determine 180 whether the certification message received satisfies the criteria for the certification requested. For example, the instructions 126 can determine whether John Doe's 172 certification message 174, alone or in combination with previously received certification messages, is sufficient to obtain Legal Department certification. If the received certification message 174 does not satisfy the criteria, the instructions 126 can store the received certification and await further certification messages. The process may store a hash for submitted content awaiting further certification to ensure that subsequent certification is for the same content as the certification already received. The process 126 can also attempt to certify any links or other objects referenced by the content (e.g., using W3C's manifest protocol).

If the received certification message satisfies certification criteria, the instructions 126 can determine 184 verification information from the certified content or other information provided. For example, the instructions 126 may compute one or more hash keys from the certified content. In general, the verification information can include any information that can be used to identify the certified content.

After storing the content's certification and verification information in the database 186, the instructions 126 can produce a digital signature 188 (e.g., a W3C DSig (Digital Signature Group) compliant signature) for the content 188. The digital signature 208 can include the computed hash 210, the content's URL 212, or any other verification or certification information (not shown).

After producing the digital signature 190, the instructions 126 can determine 190 whether the content can be dynamically modified 192 to include the digital signature. For example, HTML and XML permit dynamic insertion of

digital signatures into content (e.g., as header information or as a newly defined tag). Inclusion of the digital signature in the content ensures that the digital signature travels with the content instead of assuming the signature will remain paired with the content during distribution. The instructions 126 can also dynamically modify the content to include one or more certification indicators 106. The instructions 126 can store the digital signature(s) in its database. This prevents database contents from being tampered with as any altered database information will not match the digital signature(s) stored. Finally, the content and digital signature(s) are distributed by storage at a URL 194, 196 or by sending back the certified content to a submitting user for distribution (not shown).

Referring to FIG. 10, the certification server database 130 includes information corresponding to certified content. This information can include a URL 199, one or more hash keys 200, certifications obtained 201, the certifiers 202, and a certification expiration date 203. The database 130 can also include the location (if any) of previous 204 or later 205 content versions. When the certification server 124 receives a certification verification request, the server 124 can determine whether a user has attempted to access the most recent version of a document. The server 124 can automatically transmit the more recent version of the document to the user. The database can include a wide variety of other information 207 such as a portion of the content and/or a certification expiration date. The database 130 can also include the location of different translations of content and transmit a translation based on "Preferred Language" data included in a certification verification request.

Referring to FIG. 11, after certification, multiple digital signatures 210a, 210b of different certifications may be associated with content. The different digital signatures 210a, 210b may be encrypted and identified by an encapsulating digital signature 208 of the certification server.

Referring to FIG. 12, after content certification, the certification server 124 database 128 stores the verification information 130 corresponding to certified content 168. Referring to FIG. 13, in addition to verifying certification in response to verification requests, the certification process enables an administrator to enforce minimum certification requirements for posted content. For example, a site might define a policy that requires any content available via the World Wide Web to have certification from both the Legal and Marketing Departments. A process 300 can ensure available content meets these requirements 306 by determining the certification possessed by content at each URL 304 offered by a site. Determining content certification can include identifying and verifying digital signatures stored at the URL. Alternatively, the process 300 can determine verification information of a URL and compare the determined verification information with verification information originally stored during certification. Either technique ensures that employees or others do not post content without receiving sufficient certification.

Referring to FIG. 14, enforcing certification criteria can instead occur at a web-server processing content requests. After receiving a request for content 303, the web-server can determine 305 if the requested content has the certification required for transmission 309. If not, the web-server can notify the web-server administrator 307 that insufficiently certified content has been requested indicating that a link or directory has indicated the presence of the content on the server. This enables the administrator to quickly find content that should not be posted at the site. The web-server can also store information that specifically disavows certification for particular content.

Certification Verification

Referring to FIG. 15, in one implementation, certification instructions dynamically modify certified content to include one or more certification indicators 106a, 106b. Referring to FIG. 16, certification indicators 106c, 106d

may instead be paired with a listing of certified URLs 107c, 107d, for example, produced by a search engine. The certification indicators 106a, 106b may be packaged (e.g., included in the same ActiveX control or Java applet) with a corresponding URL 107a, 107b to prevent a certification indicator 107a, 107b from accidental or intentional pairing with a different, potentially uncertified, URL. Selecting an indicator 106, 106a, 106b can initiate a certification verification process.

Referring to FIG. 17, initiation of the certification verification process can include preparing and transmitting a certification verification request 221 to a certification server. The request 221 can include, for example, the certification claimed by a certification indicator 223 and verification information 225 determined from the content presented. The request may be encrypted to prevent analysis. The request 221 may also include a portion of the content presented 227 for comparison to similar information stored in the certification server. This can make "door-knob rattling" more difficult. That is, people wishing to find a valid hash key cannot simply submit request after request with different hash keys until one works. The request 221 can include other information such as the URL of the content, etc.

Referring to FIGS. 18-22, certification verification can be implemented in any number of ways. The techniques used to verify certification can depend in part on functions provided by the browser (or other application) presenting the content in question. For example, older browsers may not accept or be able to process digital signatures. Additionally, a browser may not include instructions for determining verification information (e.g., the ability to compute an MD5 hash from presented content).

The different certification verification techniques, nevertheless, share a general process 132. First, the procedures 132 determine verification information (e.g., computing a hash or extracting verification information from a digital signature) for content 220 being verified. When the determined

verification information matches 222, 224 the verification information originally determined during certification, the procedures 132 can conclude that the content satisfies certification criteria and has not been altered since certification. The procedures 132 may also check to ensure certification has not expired and that a more recent version of the document has not been certified.

After verifying certification, the procedures 132 can cause display of verification and/or certification information such as the entities that certified a document, when certification occurred, etc. Similarly, the procedure 132 can notify a user if verification fails. The procedures 132 can also cause other programmatic behavior to occur in addition to or in lieu of causing a display of information. A small subset of possible implementations follows.

Referring to FIG. 19, if a browser has access to digital signature(s) produced during certification and the ability to determine verification information from content, the browser can extract the verification information from the digital signature(s) 230, determine the verification information of the content in question 232, and compare the two 234. A match verifies the claimed certification 236. This method does not require access to the certification server for certification verification. However, access to the certification server enables a user to determine if the content remains certified or has been replaced by a new version.

Referring to FIG. 20, if a browser does not have access to digital signature(s) produced during certification but has the ability to determine verification information, the browser can determine the verification information for the content 240 (e.g, compute a hash) and send the determined verification information to the certification server 242. The certification server can compare 244, 246 the determined verification information with the verification information originally determined during certification. Again, if the two match, the content's certification has been verified.

Referring to FIG. 21, in some cases, content may not display a certification indicator. A user may, nevertheless, determine whether the content

received certification. In one implementation, the user can visit a certification server web-site 252 and enter a URL for verification 254. Instructions on the certification server can collect the content provided by the resource at the identified URL, determine verification information from the collected content 256, and compare the determined verification information with stored verification information of certified content. If the instructions find a match, the instructions can transmit verification and/or certification information to the user.

Referring to FIG. 22, in another implementation, a user can simply transmit content in question to the certification server 266 for certification verification. The certification server determines verification information for the content 268 and can compare 270 this verification information with verification information stored in its database. If the certification server identifies a match 272, the certification server can transmit the verification and/or certification information to a user for display 274.

Each of the implementations described above enables a user to quickly determine whether presented content actually comes from an official source. This enables a user to place greater reliance on the presented information and can make the user more likely to return to a site. The implementations also enable a content provider to closely scrutinize and guard the content it distributes.

Multiple Certification Servers

Referring to FIG. 23, the previous discussion described a single certification server. The techniques described can also be used with a network of certification servers. Certification server instructions 322 can be transmitted to different computers requesting 320 the instructions. Such transmission can occur after financial arrangements have been settled. Additionally, authentication may be performed by both the requesting and transmitting servers.

Referring to FIG. 24, certification servers may form a hierarchy 324. For example, a root certification server 326 connects to different company

"Headquarter" certification servers. For example, server 328 may belong to Honda while server 330 belongs to General Motors. Each of the headquarter servers may connect to different divisions within a company. For example, server 332 may belong to Honda Motorcycles while server 334 belongs to Honda Automobiles. Although FIG. 24 illustrates a hierarchical relationship, other certification server topologies are possible.

Hierarchically organized certification servers permit distribution of server processing and storage over a number of computers without losing the ability to verify content certified by any of the servers. Additionally, the structure permits hierarchically higher servers to control functions performed by lower servers. For example, a server can control whether another server is itself able to make a request for certification software.

For example, referring to FIG. 25, a recursive procedure 336 can quickly search each certification server to verify certification of content in question. After receiving a verification request 338, a certification server can check its own database 340 for verification information corresponding to the verification request 338. If unable to find the verification information in its own database, the server can issue a verification request to connected servers 344. Eventually, a verification request will reach the server used for certification of the content 342 or all servers will return an indication that no server has certified the content in question.

Other procedures can go up the hierarchy rather than down. For example, when a division certification server 332 receives a certification verification request it cannot provide, the division server 332 can issue a certification verification request to the headquarter's certification server 328.

Franchising

A franchisor (e.g., a corporation or syndicated) often may want to provide content for display on its franchisee's Web-sites. For example, General

Motors may want local dealerships to include a national sales advertisement. Additionally, franchisees may want to download certified content describing new products.

Referring to FIG. 26, a franchisor 350 (e.g., a corporation or syndicate) can provide content to different franchisees 352, 354. Any given site may act as both a franchisee and franchisor (not shown).

Referring to FIG. 27, after establishing a franchisor/franchisee relationship, a proxy is established at the franchisee with which the franchisor can communicate to manage content including refreshing and invalidating content. Thereafter, a franchisee can request content from the franchisor 356. After authenticating the franchisee's request 357, the franchisor can send the requested content, digital signatures associated with the content, and verification information determined for the content during certification 358. The franchisee can store the downloaded information and provide the content to site visitors 360.

Referring to FIG. 28, a franchisor can control the content offered by its franchisees. For example, to de-certify or update content, the franchisor can download replacement content or the franchisor can mark the content in the proxy invalid. When a franchisee receives a request for invalid content 364, the franchisee requests updated content from the franchisor 366. The franchisor can monitor the content offered by its franchisees by examining verification information corresponding to the content or the content itself.

After downloading information from a franchisor to a franchisee Web-server, visitors to the franchisee can view the downloaded content. The franchisee proxy can automatically transmit a certification verification request each time a visitor requests content.

Requests for content can be metered by the franchisee proxy. Thus, a franchisor can receive reports regarding which franchisee sites reached the most customers. Metering data can be used for analytical purposes or even as a way to charge for use of content (e.g., for each web-page hit) or pay for its distribution.

For example, metering can be used as a way for franchisees to charge franchisors for distribution of content, for example, by charging a small fee for each content request.

Alerting Users of Content Validation

FIG. 29 again shows a web-page 1100 presented by an Internet browser. A user viewing the page 1100 often must trust that the content-provider stands behind the contents and/or that the contents have not been tampered with. Sometimes this trust is misplaced. For example, someone may have posted the content at the business' web-site without appropriate approval (e.g., undergoing a certification process). Alternatively, some intermediate network node may have intercepted content as it traveled across the Internet and replaced selected portions.

This application describes techniques that enable a content provider to certify content. This application also describes techniques for validating certification of downloaded content. Such validation can include determining content is not certified, determining content was altered after certification, determining certification has expired, and/or determining certification has been revoked. Such validation can also include determining and authenticating the identities of entities claiming to have certified the content. As shown in FIGS. 30-36, these techniques have been embodied in a software program that can use graphical indicators, sound, and other notification techniques to notify a user whether downloaded content is certified content.

Display of Certification Status

A number of different mechanisms can notify users of whether downloaded content is certified content. For example, FIGS. 30 and 31 show a Microsoft® Windows 95 taskbar button 1104 and tray icon 1106 that change appearances based an attempt to validate certification of content displayed in an

active browser window. For example, the controls 1104, 1106 may notify a user of the certification status (e.g., certified, uncertified, expired, revoked, etc.) of content using text, graphics, color, and other display attributes. The appearance of the controls 1104, 1106 may vary in different ways for different certification statuses. For example, content that was never certified may cause the tray icon to display a bright red skull and cross bones to alert a user, while content having revoked certification may cause the tray icon to turn orange. The unobtrusive placement of the controls 1104, 1106 provides real-time, continual, notification of content certification without interfering with a user's normal browser interaction.

FIGS. 32-35 show a number of other user notification techniques. For example, FIG. 28 shows a window 1108 that displays a map 1110 of content displayed by a browser. The map 1110 may include a logo (not shown) of the site offering the content. The different appearances of map regions indicate the certification status of content. For example, red portions may indicate uncertified regions of a page, while white portions may indicate certified regions. The window enables a user to quickly identify potentially uncertified content.

FIG. 33 shows a window 1112 that displays a tree of web-page contents 1114-1120. Each node in the tree can correspond to a different content (e.g., a node for a page's HTML and nodes for different GIF (Graphics Interchange Format) pictures referred to by the page). Again, different display attributes of tree nodes reflect the certification status of content. For example, shaded node 1116 indicates that the picture for "Digests of Patent Opinions Federal Circuit" has not been certified. The map of FIG. 32 and the tree of FIG. 33 can provide a user with a visual description of content certification, without altering the browser's display of the page or otherwise altering the browser's functions.

Other techniques, however, use browser-provided functions to provide an indication of the certification status of content. For example, as shown in FIG.

34, a browser may be dynamically programmed to display the certification status of content on a page as a user brushes the content with a cursor. For browsers not offering this capability, this feature may be offered by continuously determining cursor placement and displaying a window near the content. Alternatively, the window may only be displayed when a user selects content, for example, by clicking a mouse button on the content.

As shown in FIG. 35, software can also directly alter the display of contents after determining the certification of different portions. For example, as shown, the software can black-out 1114 uncertified content, and/or alter the display of content 1116 having expired certification. Depending on the browser, this may require writing a downloaded page to a temporary file, modifying the temporary file, and reloading the modified temporary file into the browser.

The embodiments described above can also provide more detailed information about the certification of content. For example, by selecting the system taskbar button 1104 in FIGS. 30 or 31, a dialog, as shown in FIG. 36, can display detailed information about content. The detailed information can include the certifying entity 1124, a graphic for the entity (e.g., a business trademark), the trustworthiness of the page or content 1125, the URL (Universal Resource Locator) or URI (Universal Resource Indicator) of the content 1127, the range of dates the certification is valid 1128, and a "digital fingerprint" of the content 1129. The dialog may also display other information (not shown) such as the site certificate of the web-site providing the page and potentially a text description of the "Trust Policy" used by the site to certify content (e.g., "Factpoint, Inc. uses a five person review board to certify content prior to posting").

Any of the visual techniques described above can be combined and/or used in conjunction with non-visual techniques such as audio messages (e.g., "The picture of Abe Lincoln is untrustworthy"). Additionally, while the above description described individual pages, the same techniques work equally well with framed browser displays that display two or more pages simultaneously.

Underlying the displays shown in FIGS. 30-36 are certification procedures that enable providers to certify posted content and validation procedures that enable users to validate the certification of received content.

The Trust Validator

FIG. 37 shows a client 1136 browser 1140 downloading information (i.e., page 1132) from a URL (Universal Resource Locator) 1132 over a network 1144. The client 1136 can present the downloaded content on a user's monitor 1142, speaker, etc. As shown, the client 1136 includes "trust validator" software 1138 that validates certification of downloaded content. The validator 1138 may operate as a background process that monitors content received by the browser 1140, for example, via calls to or from the browser API (application programming interface). Alternatively, validator 1138 functions may be directly integrated into the browser 1140.

The validator 1138 can validate content certification using certification information associated with the content. For example, the validator 1138 can compare certification information determined for the content determined prior to transmission to the client with certification information determined after transmission.

In more detail, a certification process produces certification information 1134 based on the certified content(s). Typically, this information 1134 is produced using a "one-way" function. For example, a hashing function may use all or some portion of the ASCII characters in HTML (HyperText Markup Language) commands that define a page to produce a set of output bytes. Given the same input, the hashing function produces the same output. A popular hashing functions known as MD5 and SHA can produce relatively small output for large pages.

The certification information 1134 derived from the content may be included in the content itself, for example, as data, for example, as signature

and/or manifest elements of an XML (Extensible Markup Language) page or as an HTML "Meta" element. When the certification information 1134 is included in the content, it must be removed before re-determining the certification information.

Alternatively, the information 1134 may be included in the header of an HTTP (HyperText Transfer Protocol) message sent by the server 1130. In yet another implementation, the trust validator 1138 may independently request certification information 1134 for the downloaded content. For example, the site may provide a file (e.g., "factpoint.txt") at a predefined location (e.g., "www.url.com/factpoint.txt") that lists where certification information 1134 for site content can be found. The file may refer to other sites when the content has been copied.

FIG. 38 shows a process 1138 the trust validator can use to validate certification of downloaded content. First, the trust validator obtains 1150 the downloaded content (e.g., a page or portion of a page) and the certification information associated with the content. The trust validator 1138 can obtain this information from the browser 1140 or can establish an independent connection with the server 1130. The trust validator 1138 can independently determine certification information using 1152 the one-way function on the received content. By comparing 154 the received certification information and the independently determined certification information, the validator 1138 can determine 1154 whether the page 1132 has been altered since certification and notify a user of such a change. The trust validator may also notify a web-site administrator if certification validation fails so the administrator can investigate uncertified content offered by the site.

FIG. 39 shows a scheme that can not only detect tampering, but that can also identify and authenticate the entity or entities certifying content. This scheme features certification information that includes a hash digitally signed by one or more certifying entities. A digital signature 1160, much like a handwritten

signature on a piece of paper, provides a degree of certainty that a particular entity signed the content in question.

One digital signature scheme uses a private encryption key known only to the signer and a public encryption key that may be freely distributed. Information encrypted with the private key can only be unencrypted with the public key. Thus, an entity certifying content can encrypt a hash of the content with their private key. Only the public key associated with the entity can properly decrypt the hash. For example, a hash of content may be encrypted using a private key assigned to a web-site and decrypted using a public key included in the site's certificate. A wide variety of other digital signature schemes may be used such as an exchange of a single encryption key or the use of physical devices such as smart cards.

In the system of FIG. 39, information needed to validate a digital signature may be included with the certification information. The information may include an X.509 certificate for each entity signing the hash. For example, an X.509 certificate may include the public key needed to decrypt the hash of the page 1132, a description of the entity holding the private key, and the digital signature of some authority such as VeriSign® testifying to the truth of the information in the certificate (i.e., that the entity claiming to have signed the hash is actually the claimed entity). In another embodiment, the information needed to validate a digital signature (or a reference to this information) may be provided by one or more DSig (Digital Signature Users Group) digital signature blocks.

As shown in FIG. 40, after receiving the certification information (e.g., digital signature and certificates), the trust validator 1138 can use the public key included in the certificate to extract the hash included in the digital signature. The trust validator 1138 can also follow the chain of authority 1162, for example, by asking VeriSign® if the public key received is really the public key of the entity claiming to have signed the hash. The trust validator can include information about the chain of authority in a display such as the dialog shown in

FIG. 36. After extracting the hash from the certification information, the trust validator 1138 can conclude the page was altered or was never certified to begin with and can notify a user using the techniques described above.

If the certification information includes a digitally signed hash, the certification information may be transmitted over an insecure connection. If, however, the certification information only includes a hash, a secure connection such a secure sockets layer (SSL) connection may be preferred.

As shown in FIG. 41, instead of a single digital signature or hash, certification information may include a manifest 1170 for content included in a page. The manifest 1170 itself may be hashed and digitally signed. As shown in FIG. 42, the manifest 1170 can include the hash values of different page 1130 content. For example, the manifest 1170 shown includes a different hash value for each picture displayed on the page. The trust validator 1138 can use this information to validate each portion of a page individually. The validator 1138 can also use criteria to produce an overall estimation of page certification. This criteria may be provided by rules included in the manifest 1170 (e.g., defining valid content collections), logic hard-coded into the validator, and/or as logic provided by user-supplied code (e.g., a Java script). By default, the validator 1138 can describe the page as having the lowest certification status of any content in the page. For example, if any content on the page has expired, the page as a whole is deemed expired. The validator 1138 may use similar logic for frames. That is, the overall certification status of a display is determined by the worst certification status of any content in any displayed frame.

In some implementations, the trust validator 1138 can alert a user to revocation, expiration, and other certification statuses of downloaded content. FIG. 43 shows a server 1130 that includes a database table 1182 describing available content 1132. The table 1182 can include an expiration date for certification, a blanket revocation of certification, and other information. Upon receiving content, the trust validator 1138 can transmit a validation request to

validation software 1180 on the server 1130. The validation software 1132 can access the table 1182 to verify the content was certified and determine whether the content has expired or has been revoked. The validation software 1132 can transmit the results back to the trust validator 1138.

Though information in the table 1182 may be included in the certification information received by the client, the table 1182 enables an administrator to centrally alter certification information. The server table 1182 can also be used to provide content "versioning". For example, a web-site may certify a more recent version of information for a URL. Validation software can look for valid versions of a URL when a client attempts to validate expired or revoked content.

FIG. 44 describes this validation process in greater detail. After receiving the content and its corresponding certification information 1200 and independently determining the certification 1204 for the content, the validator 1138 can preliminarily determine if the content is certified without accessing the server 1130. For additional validation, the validator 1138 can also transmit 1206 certification information (e.g., the hash) to the server validation software for look-up in the server table 1182. The server table 1182 can not only verify that the content has not expired or been revoked, the server table 1182 can also identify more recent content that replaces the content the user downloaded (e.g., the URL for the hash submitted has another table entry that has not been revoked). The trust validator can then establish a connection to download the valid version for display in the browser.

FIG. 45 shows a secure architecture that distributes server certification and validation functions between a certification server 1218 and a validation server 1232. The certification server 1218 includes certification software 1220 that certifies submitted content 1214. The certification server 1218 also adds table 1182 entries as content is certified.

An administration tool 1216 can manage information stored in the table, for example, to specify an expiration date, delete certification, or revoke certification for content.

The certification software 1220 may certify a single piece of content or a collection of web-pages using a certification "spider." Certification may be performed for fixed or dynamically constructed content. After certification, the certification server can place certified content on the validation server for distribution.

The validation server 1232 includes validation software 1228 that accesses the certification server 1220 table 1182 in response to client validation requests. The validation server 1232 may maintain a cache of validation data to reduce the time spent serving client requests.

Embodiments

The techniques described here are not limited to any particular hardware or software configuration; they may find applicability in any computing or processing environment. For example, functions described as being performed by a certification server can be distributed across different platforms.

The techniques may be implemented in hardware or software, or a combination of the two. Preferably, the techniques are implemented in computer programs executing on programmable computers that each include a processor, a storage medium readable by the processor (including volatile and non-volatile memory and/or storage elements), at least one input device, and one or more output devices. Program code is applied to data entered using the input device to perform the functions described and to generate output information. The output information is applied to one or more output devices.

Each program is preferably implemented in a high level procedural or object oriented programming language to communicate with a computer system.

however, the programs can be implemented in assembly or machine language, if desired. In any case, the language may be a compiled or interpreted language.

Each such computer program is preferably stored on a storage medium or device (e.g., CD-ROM, hard disk or magnetic diskette) that is readable by a general or special purpose programmable computer for configuring and operating the computer when the storage medium or device is read by the computer to perform the procedures described in this document. The system may also be considered to be implemented as a computer-readable storage medium, configured with a computer program, where the storage medium so configured causes a computer to operate in a specific and predefined manner.

Other embodiments are within the scope of the following claims.

What is claimed is:

1. A method of processing content, comprising:

storing verification information corresponding to certified content at a first computer;

receiving a verification request corresponding to content from a second computer;

determining verification information for the content corresponding to the verification request; and

comparing the determined verification information with the stored verification information.

2. The method of claim 1, further comprising, receiving content certification criteria.

3. The method of claim 2, wherein certified content comprises content satisfying the content certification criteria.

4. The method of claim 2, wherein content certification criteria comprises a list of required approval.

5. The method of claim 2, wherein content certification criteria comprises programmed logic.

6. The method of claim 1, further comprising storing certification information.

7. The method of claim 6, wherein certification information comprises at least one of the following: a type of certification granted, entities approving certification, and when the content was certified.

8. The method of claim 1, wherein verification information comprises information derived from the content.

9. The method of claim 8, wherein information derived from the content comprises at least one hash key.

10. The method of claim 1, wherein the verification request includes a URL (Uniform Resource Locator).

11. The method of claim 10, wherein determining verification information comprises collecting content from the URL included in the verification request.

12. The method of claim 1, wherein the verification request includes content.

13. The method of claim 12, wherein determining verification information comprises determining verification information for the content included in the verification request.

14. The method of claim 1, wherein the verification request includes verification information.

15. The method of claim 14, wherein determining verification information comprises using the verification information included in the verification request.

16. The method of claim 1, wherein receiving a verification request comprises receiving a request caused by user interaction with a certification indicator.

17. The method of claim 16, wherein the certification indicator is included in the content.

18. The method of claim 16, wherein the certification indicator comprises a graphic image having associated instructions that produce a verification request.

19. The method of claim 1, further comprising transmitting certification information to the second computer.

20. The method of claim 1, wherein the content comprises at least one of the following: graphics, text, animation, sound, and instructions.

21. The method of claim 1, wherein the content comprises a web-page.

22. The method of claim 1, wherein comparing comprises issuing verification requests to connected certification servers.

23. A method, comprising:

presenting an indication that content has received certification;

receiving user input requesting verification that the content has received the certification indicated;

transmitting a certification verification request to a certification server; and

receiving information describing whether the content has actually received the certification presented by the indication.

24. The method of claim 23, wherein presenting an indication comprises presenting a user interface control.

25. The method of claim 24, wherein receiving user input comprises receiving user input via the user interface control.

26. The method of claim 23, further comprising displaying information included in the information received.

27. The method of claim 23, wherein the information received comprises at least one of the following: content authorship, revision number, expiration date, and type of certification.

28. The method of claim 23, wherein transmitting a certification verification request comprises transmitting verification information determined from the content.

29. The method of claim 28, wherein the verification information comprises a hash key.

30. The method of claim 23, wherein transmitting a certification verification request comprises transmitting information included in the content.

31. The method of claim 23, wherein transmitting a certification verification request comprises transmitting a URL.

32. A method of controlling content distribution, comprising:

receiving certification requirements for content to be distributed;

identifying content to be distributed; and

determining whether the identified content satisfies the received certification requirements.

33. The method of claim 32, wherein identifying content comprises receiving a request for content.

34. The method of claim 32, wherein identifying content comprises collecting content from a set of locations.

35. The method of claim 32, wherein the determining comprises identifying at least one digital signature associated with the content.

36. The method of claim 32, wherein the determining comprises determining verification information for the content.

37. A method of processing content received from a networked computer in response to a browser request for content, the method comprising:

receiving certification information associated with content received by the browser;

determining a certification status for content based on the received certification information; and

displaying at least one indication of the determined certification status of the content.

38. The method of claim 37, wherein the indication comprises a persistant indication displayed with the content.

39. The method of claim 37, wherein the indication comprises a taskbar button.

40. The method of claim 37, wherein the indication comprises a tray icon.

41. The method of claim 37, wherein displaying at least one indication comprises processing the content to include one or more indications.

42. The method of claim 41, wherein processing the content comprises altering visual representation of the content.

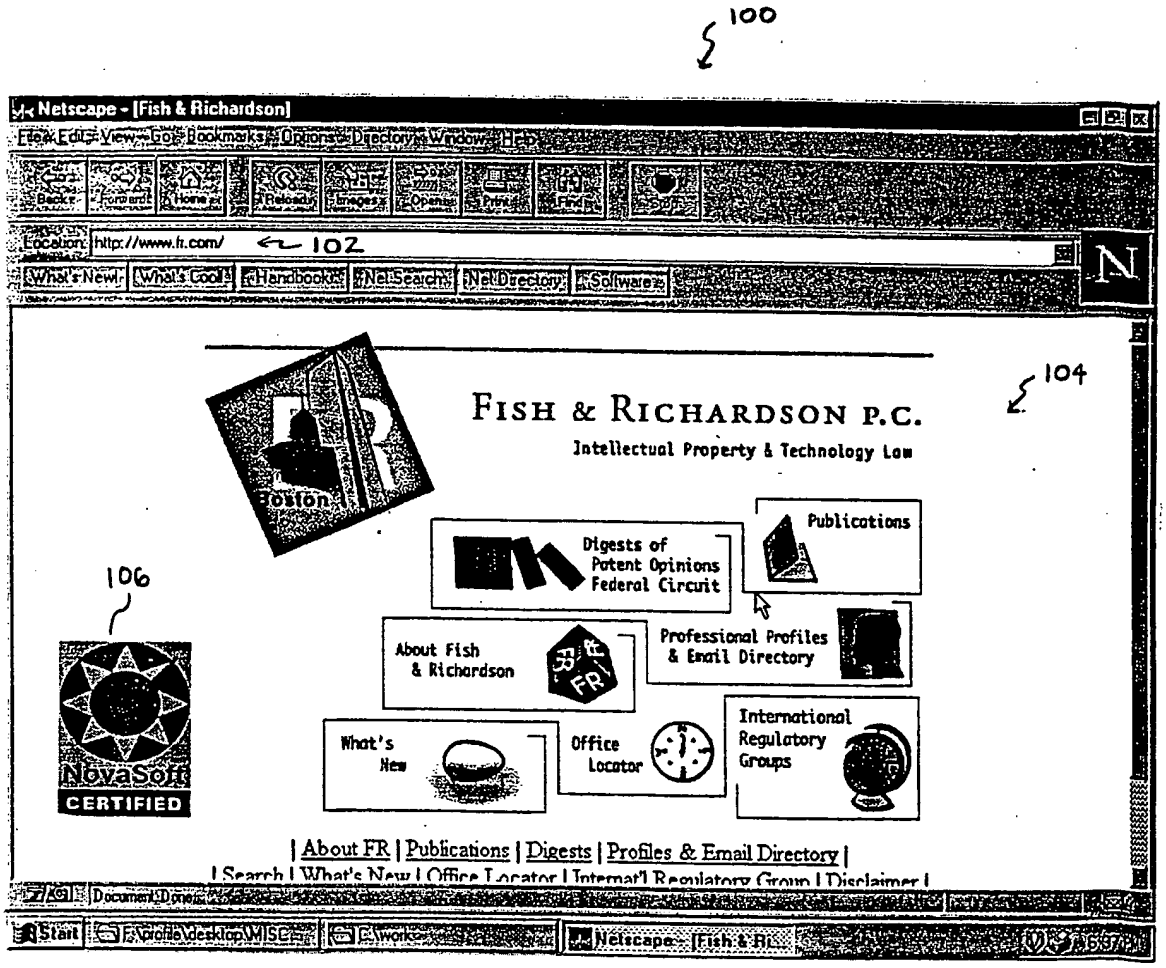

100
Netscape - [Fish & Richardson]
Location: http://www.fr.com/
102
What's New!
What's Cool!
Handbooks
Net Search
Net Directory
Software
FISH & RICHARDSON P.C.
Intellectual Property & Technology Law
104
Publications
Digests of Patent Opinions Federal Circuit
About Fish & Richardson
Professional Profiles & Email Directory
What's New
Office Locator
International Regulatory Groups
106
NovaSoft
CERTIFIED
| About FR | Publications | Digests | Profiles & Email Directory |
Start

FIG. 1

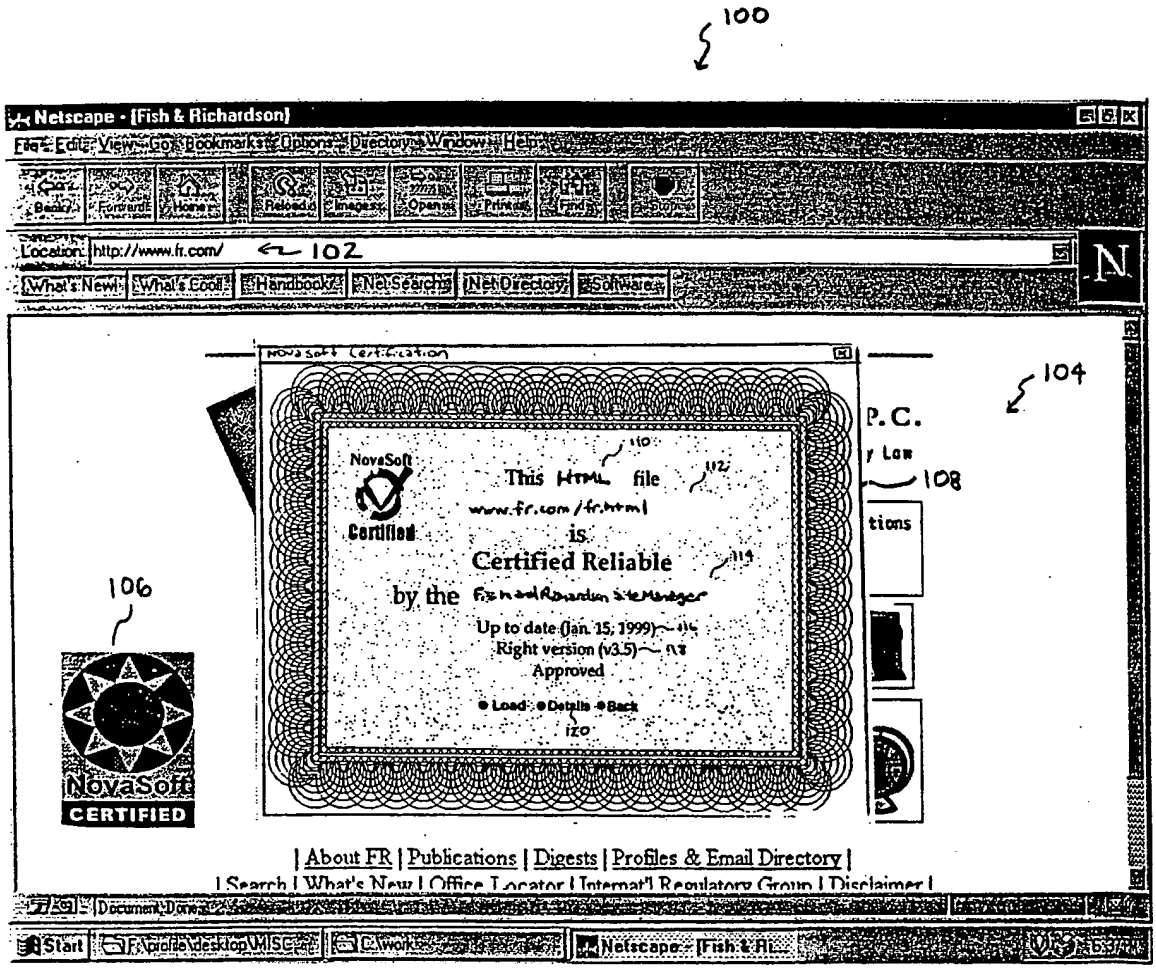

100
Netscape - [Fish & Richardson]
Location: http://www.fr.com/
102
What's New!
What's Cool!
Handbook
Net Search
Net Directory
Software
104
P.C.
108
NovaSoft
Certified
This HTML file
www.fr.com/fr.html
is
Certified Reliable
by the
Up to date (Jan. 15, 1999)
Right version (v3.5)
Approved
Load
Details
Back
106
NovaSoft
CERTIFIED
About FR | Publications | Digests | Profiles & Email Directory |
Start
Netscape - [Fish & R...

FIG. 1

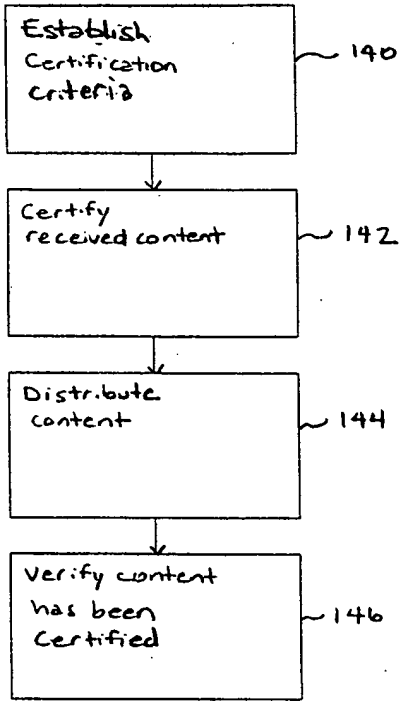

Establish Certification criteria
140
Certify received content
142
Distribute content
144
Verify content has been Certified
146

FIG. 3

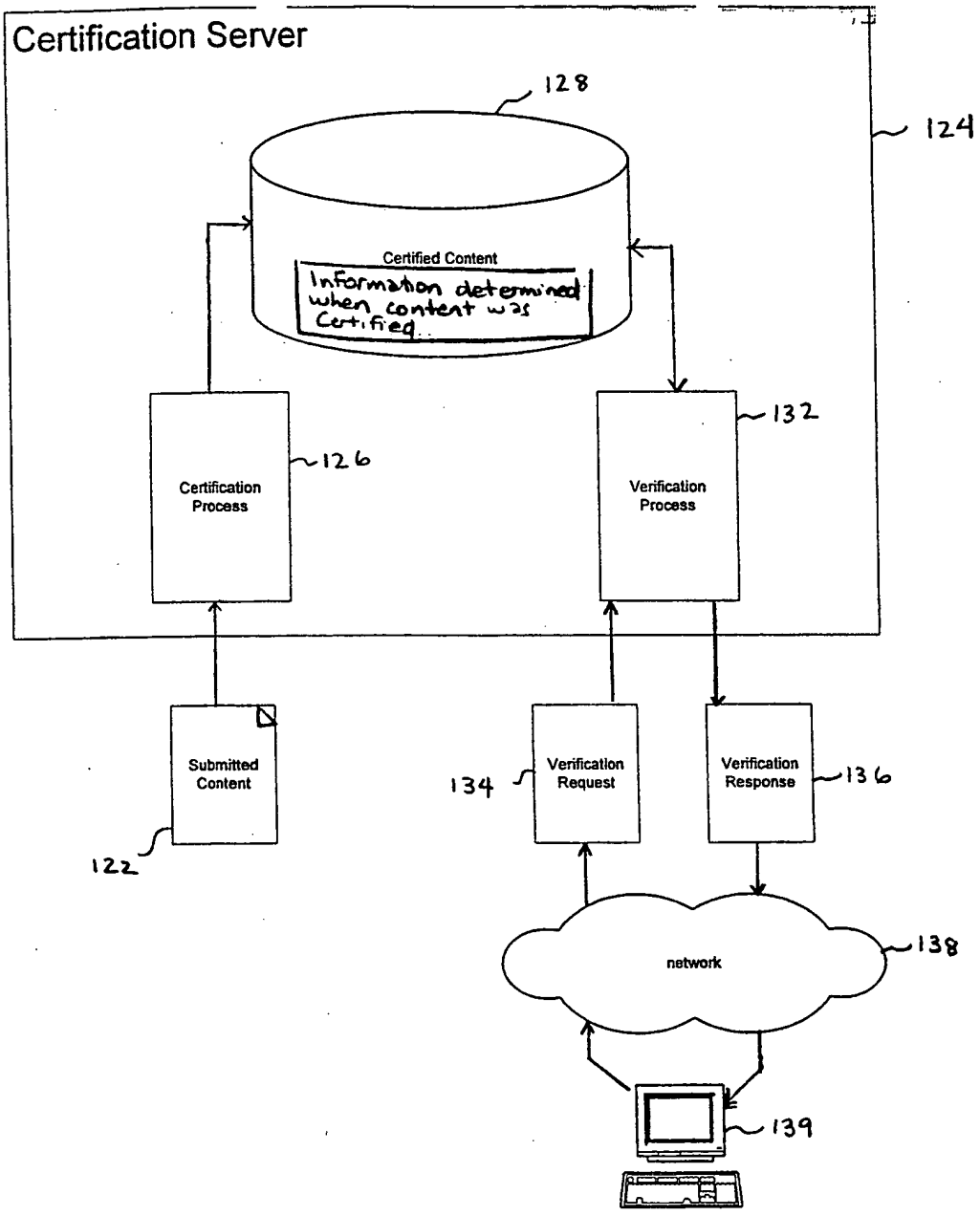

Certification Server
128
124
Certified Content
Information determined when content was Certified
Certification Process
126
Verification Process
132
Submitted Content
122
134
Verification Request
Verification Response
136
network
138
139

FIG. 4

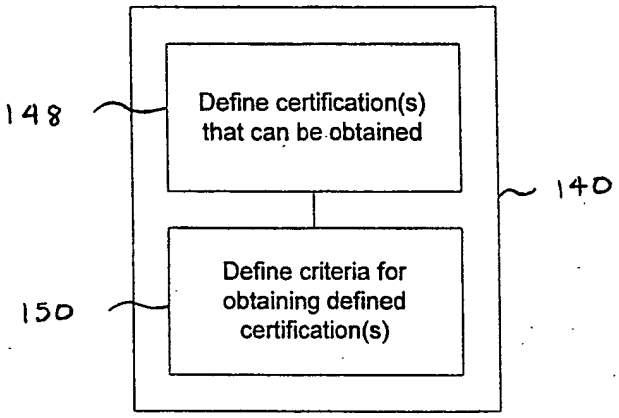

148
Define certification(s) that can be obtained
140
150
Define criteria for obtaining defined certification(s)

FIG. 5

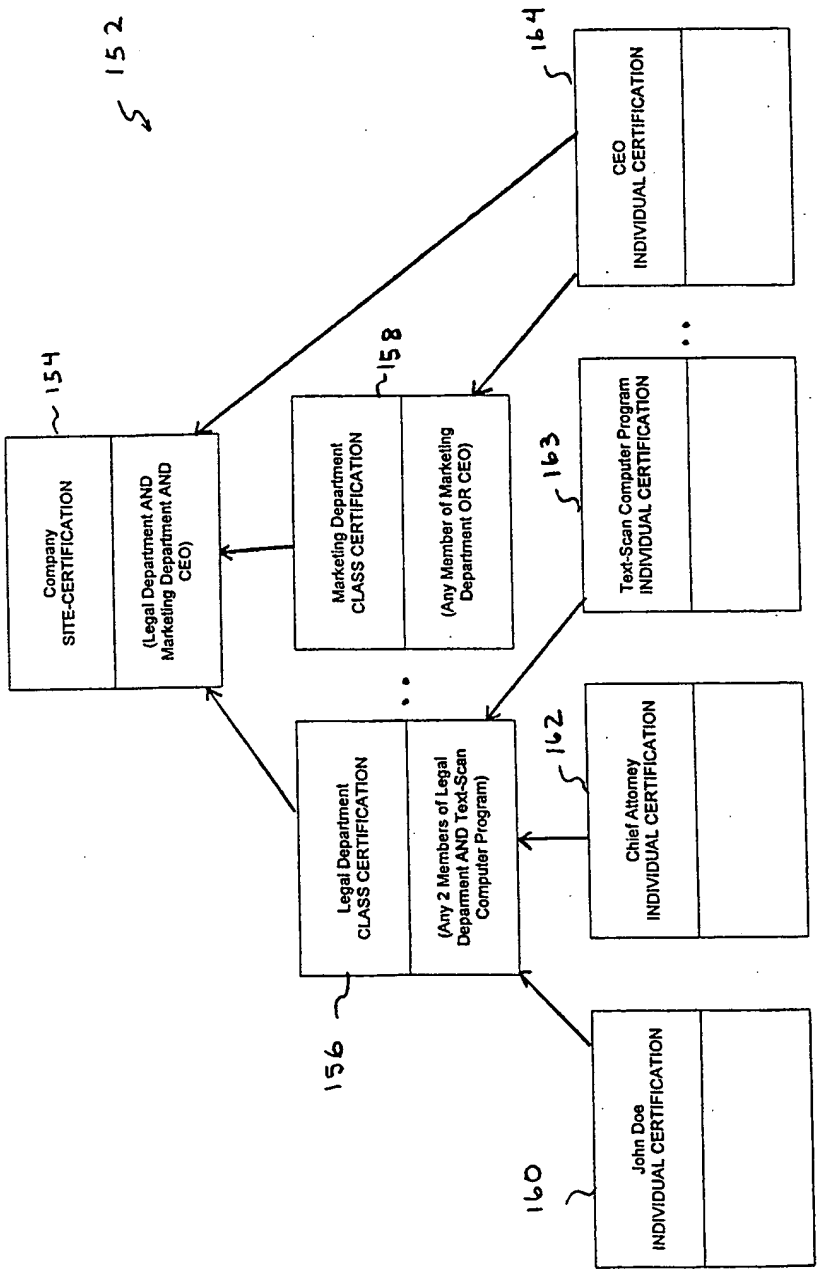

152
154
Company
SITE-CERTIFICATION
(Legal Department AND
Marketing Department AND
CEO)
158
Marketing Department
CLASS CERTIFICATION
(Any Member of Marketing
Department OR CEO)
164
CEO
INDIVIDUAL CERTIFICATION
163
Text-Scan Computer Program
INDIVIDUAL CERTIFICATION
162
Legal Department
CLASS CERTIFICATION
(Any 2 Members of Legal
Deparment AND Text-Scan
Computer Program)
Chief Attorney
INDIVIDUAL CERTIFICATION
156
160
John Doe
INDIVIDUAL CERTIFICATION

FIG. 6

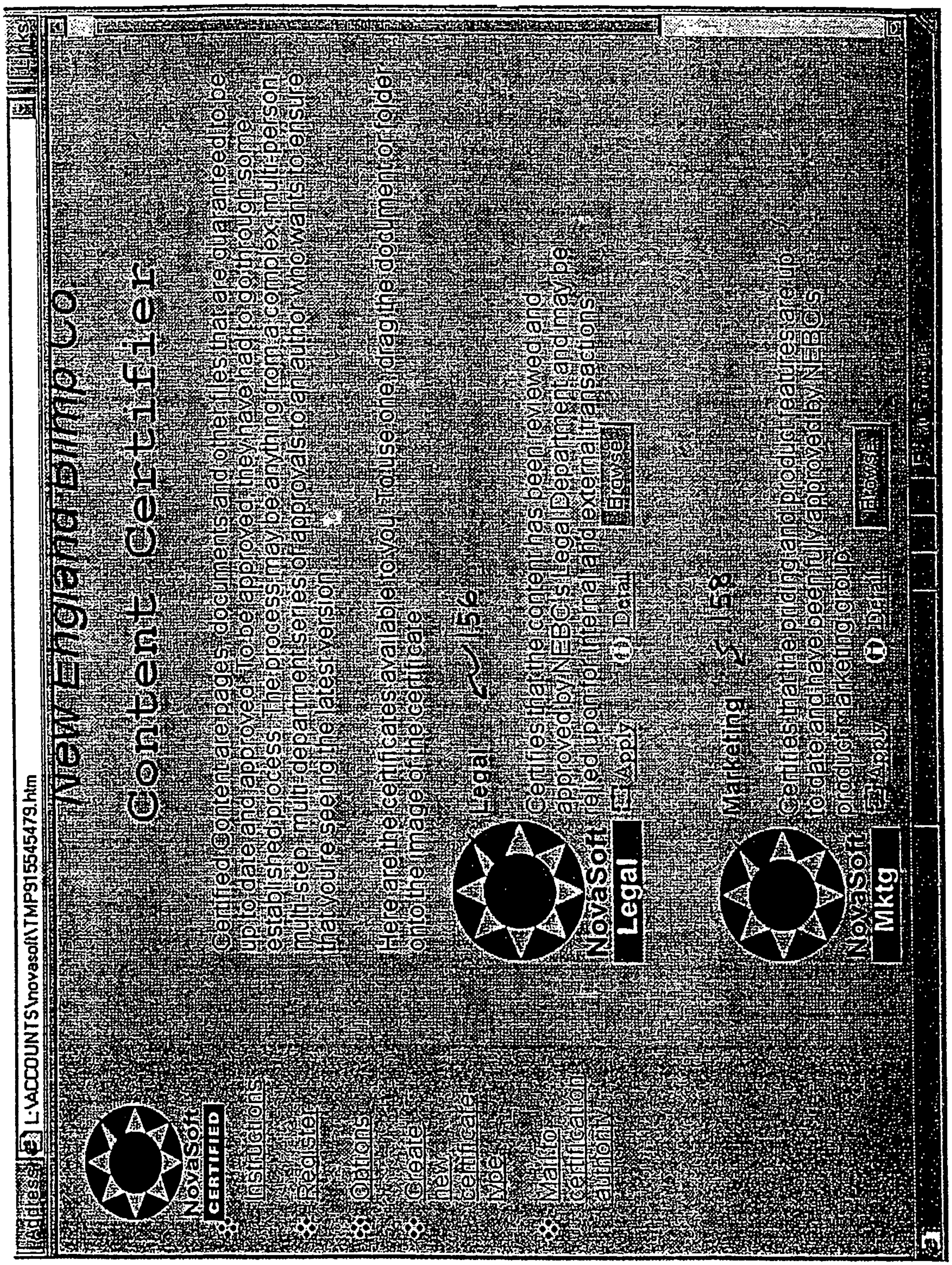

L:\ACCOUNTS\novasoft\TMP915545479.htm
New England Blimp Co.
Content Certifier
Legal
Marketing
Browse
Legal
Mktg
NovaSoft
CERTIFIED
156
158

FIG. 7A

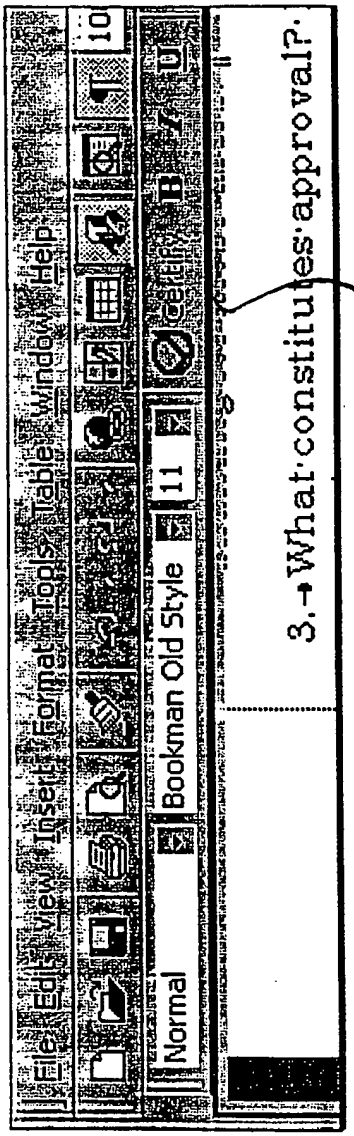
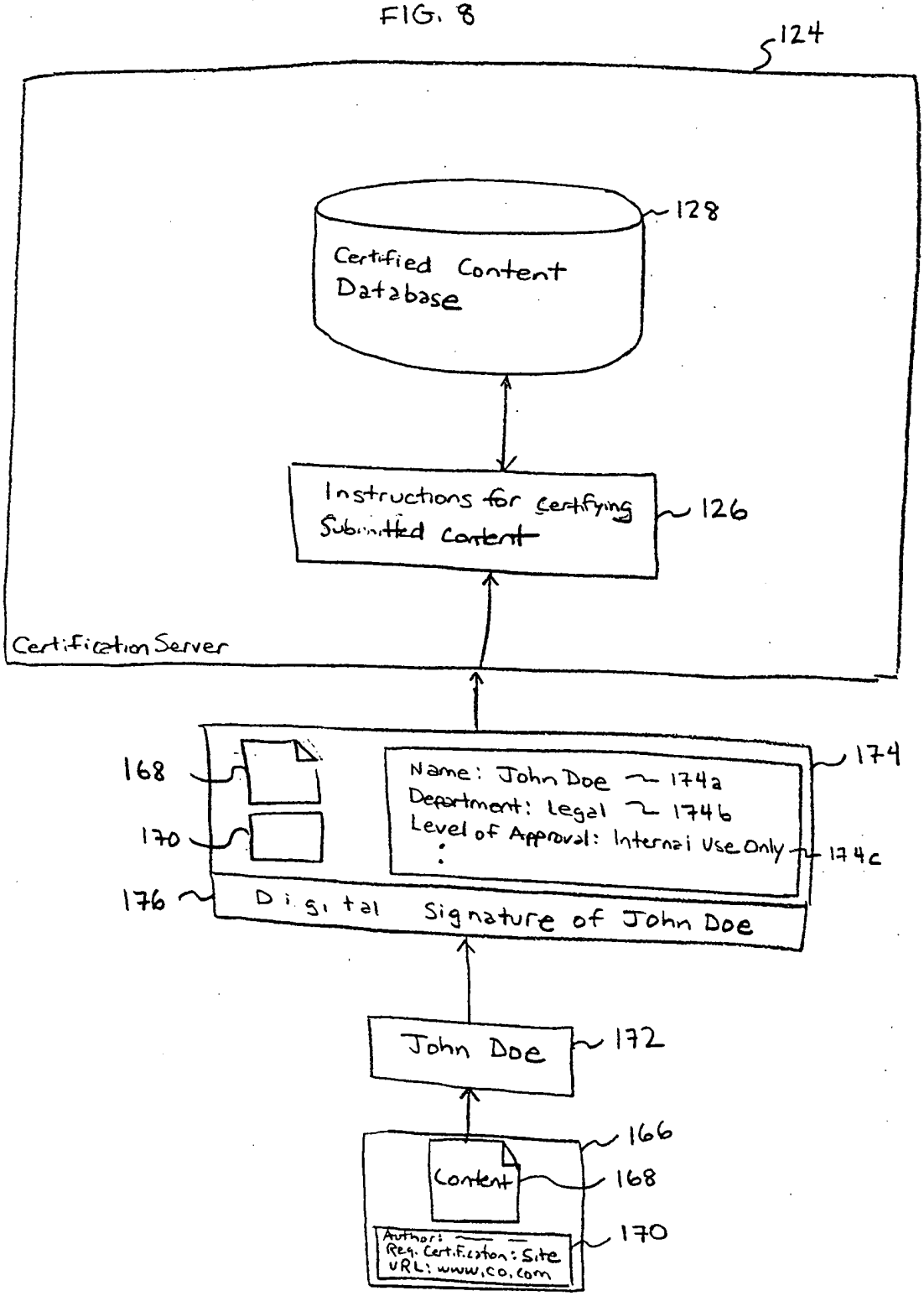

File Edit View Insert Format Tools Table Window Help
Normal
Bookman Old Style
11
3. What constitutes approval?
171
173

FIG. 7B

FIG. 8


124
128
Certified Content Database
Instructions for certifying Submitted Content
126
Certification Server
168
170
Name: John Doe 174a
Department: Legal 174b
Level of Approval: Internal Use Only 174c
174
176
Digital Signature of John Doe
John Doe
172
166
Content
168
Author:
Req. Certification Site URL: www.co.com
170

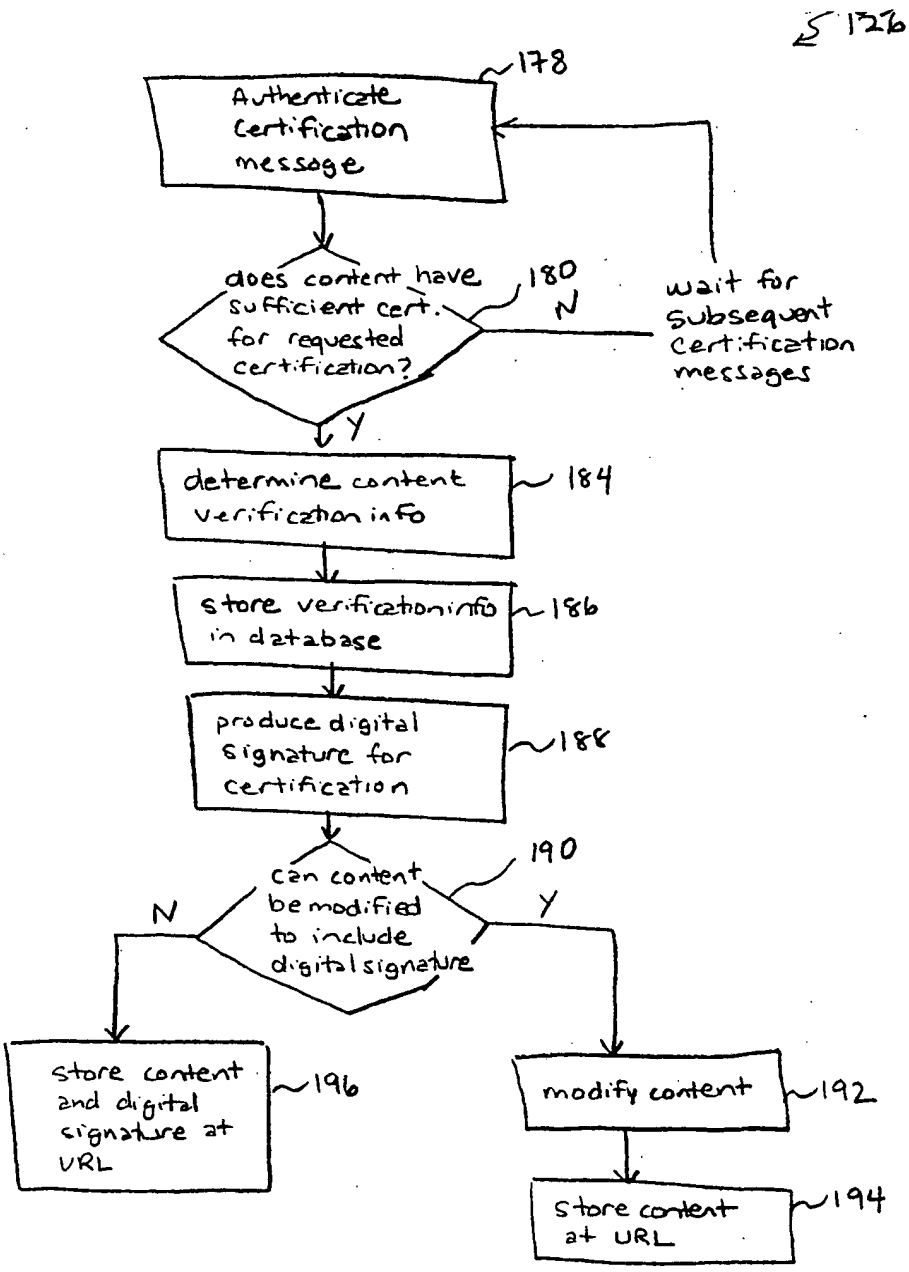

176
178
Authenticate certification message
does content have sufficient cert. for requested certification?
180
N
wait for subsequent certification messages
Y
determine content verification info
184
store verification info in database
186
produce digital signature for certification
188
can content be modified to include digital signature
190
N
Y
store content and digital signature at URL
196
modify content
192
store content at URL
194

FIG. 9

URL (199)	Hash(es) (200)	Certification(s) (20.)	Approver(s) (202)	Expiration Date (203)	Previous Version (204)	Newer Version (205)	Valid (206)	... (207)
www.co.com/a.html	FDFAE938 0C8	Legal Dept	John Doe Chief Attorney Text Scan	12/31/91	www.co.com/a-old.html	www.co.com/a-new.html	Yes	..

130

FIG. 10

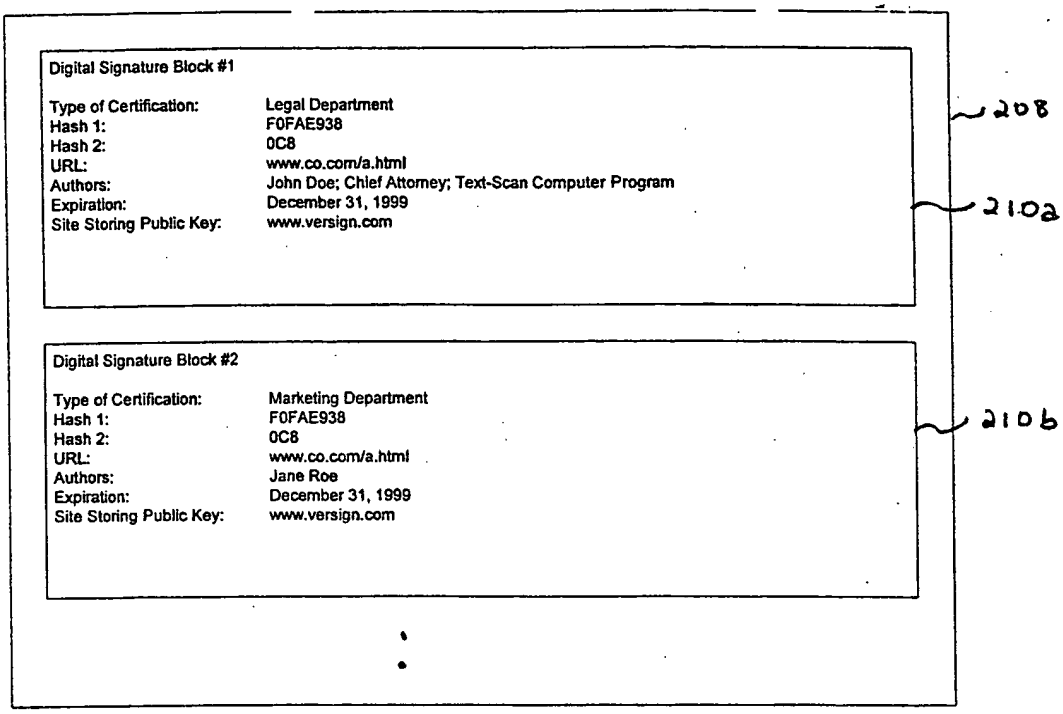

Digital Signature Block #1
Type of Certification: Legal Department
Hash 1: F0FAE938
Hash 2: 0C8
URL: www.co.com/a.html
Authors: John Doe; Chief Attorney; Text-Scan Computer Program
Expiration: December 31, 1999
Site Storing Public Key: www.versign.com
208
210a
Digital Signature Block #2
Type of Certification: Marketing Department
Hash 1: F0FAE938
Hash 2: 0C8
URL: www.co.com/a.html
Authors: Jane Roe
Expiration: December 31, 1999
Site Storing Public Key: www.versign.com
210b

FIG. 11

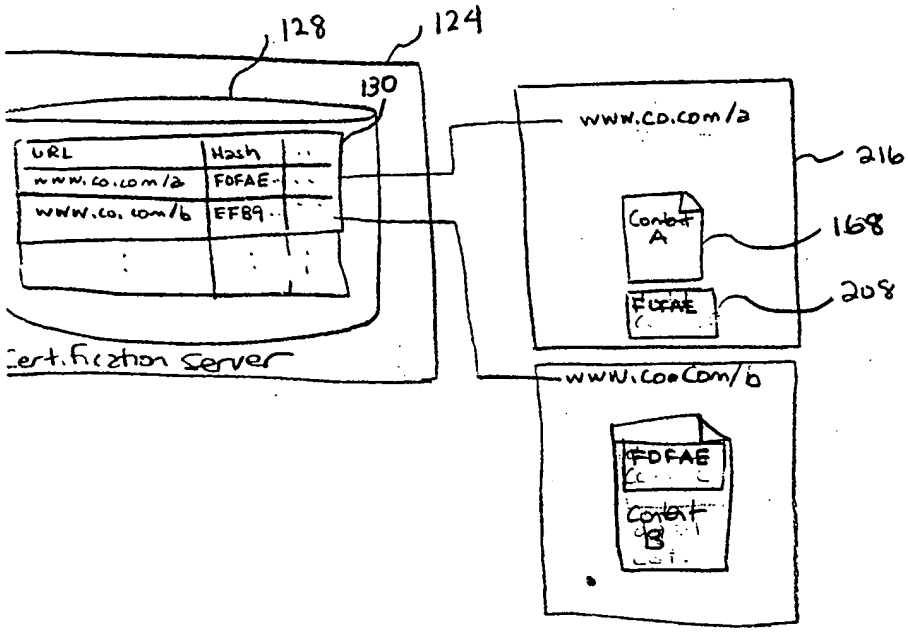

128
124
130
URL
Hash
www.co.com/a
F0FAE
www.co.com/b
EFB9
Certification Server
www.co.com/a
216
Content A
168
FOFAE
208
www.co.com/b
FDFAE
Content B

FIG. 12

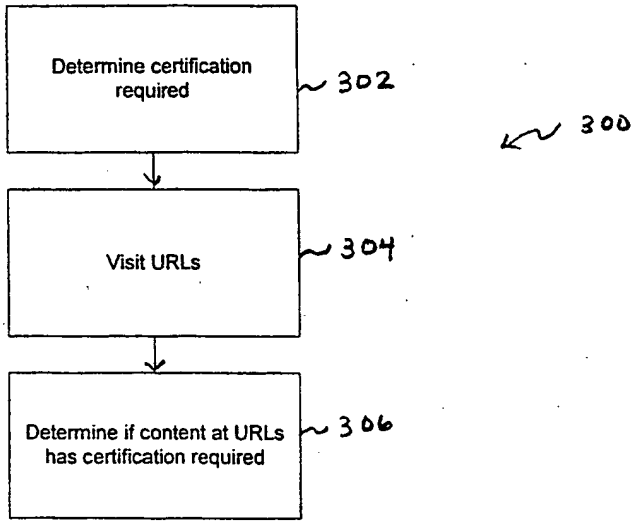

Determine certification required
302
300
Visit URLs
304
Determine if content at URLs has certification required
306

FIG. 13

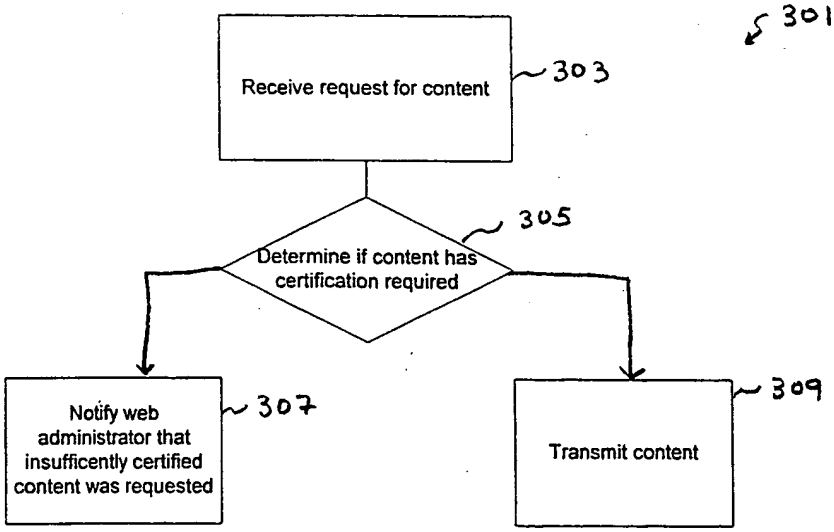

301
Receive request for content
303
305
Determine if content has certification required
Notify web administrator that insufficently certified content was requested
307
Transmit content
309

FIG. 14

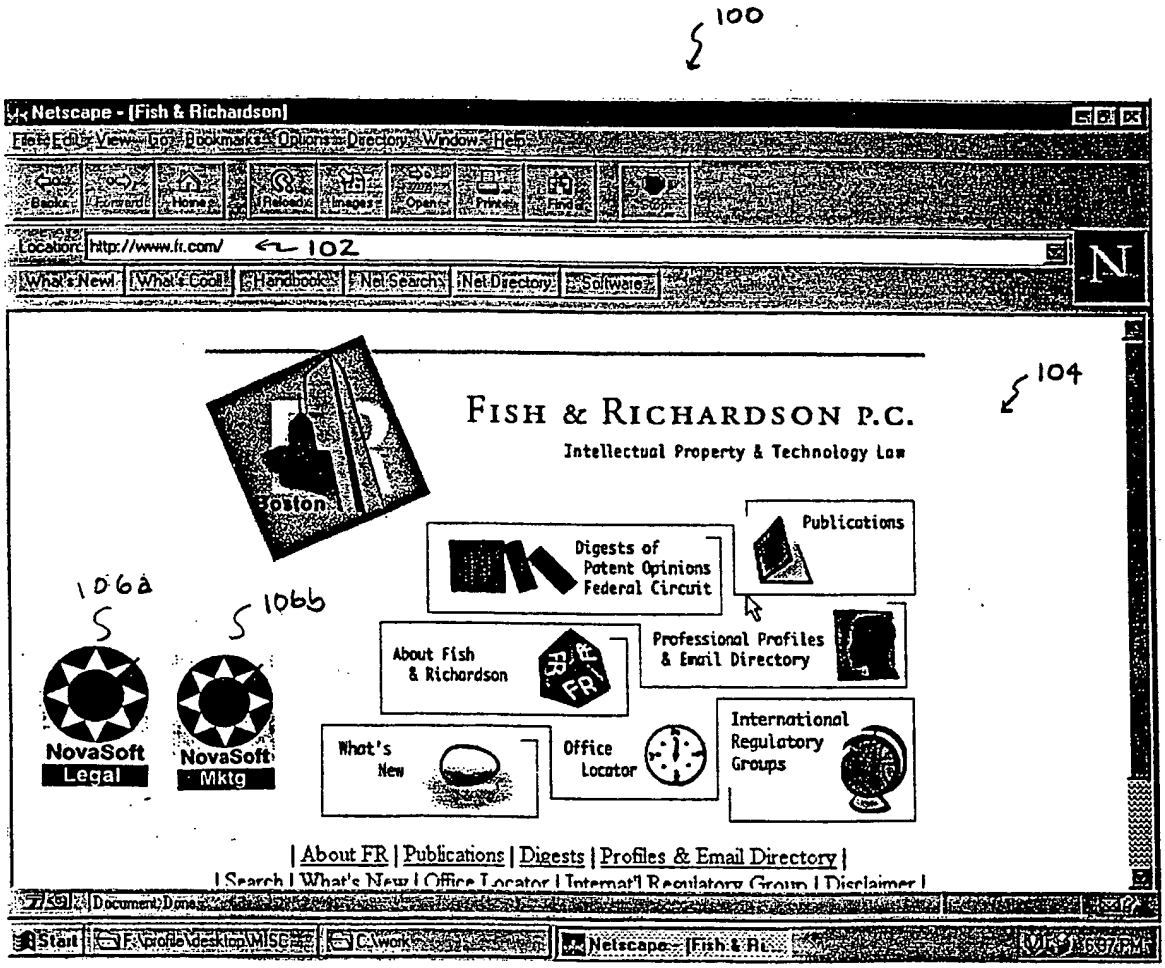

100
Netscape - [Fish & Richardson]
File Edit View Go Bookmarks Options Directory Window Help
Back Forward Home Reload Images Open Print Find Stop
Location: http://www.fr.com/
102
What's New! What's Cool! Handbook Net Search Net Directory Software
104
FISH & RICHARDSON P.C.
Intellectual Property & Technology Law
Boston
Digests of Patent Opinions Federal Circuit
Publications
About Fish & Richardson
Professional Profiles & Email Directory
What's New
Office Locator
International Regulatory Groups
106a
106b
NovaSoft Legal
NovaSoft Mktg
| About FR | Publications | Digests | Profiles & Email Directory |
| Search | What's New | Office Locator | Internat'l Regulatory Group | Disclaimer |
Document Done
Start
Netscape - [Fish & Ri...

FIG. 15

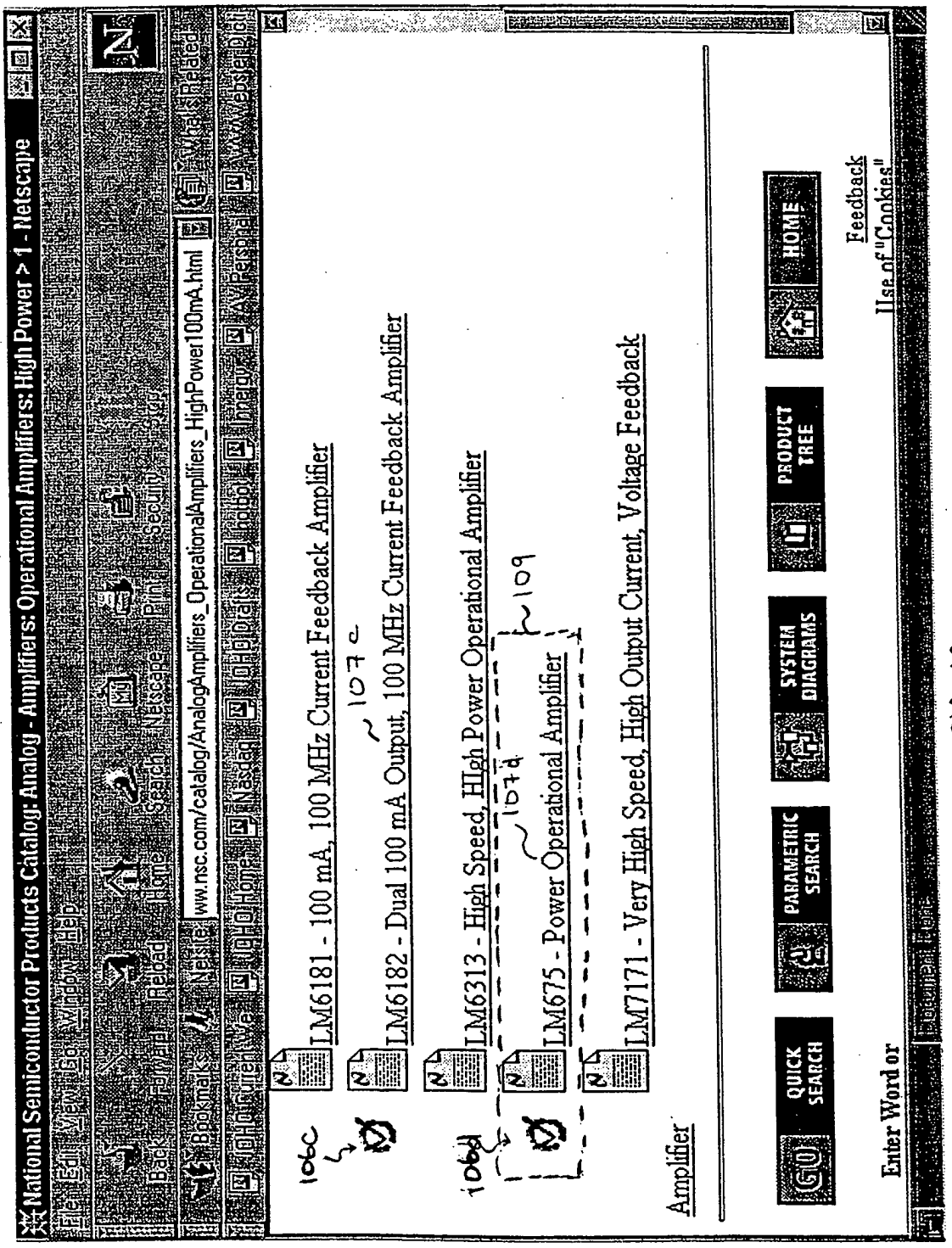

National Semiconductor Products Catalog: Analog - Amplifiers: Operational Amplifiers: High Power > 1 - Netscape
www.nsc.com/catalog/AnalogAmplifiers_OperationalAmplifiers_HighPower100mA.html
LM6181 - 100 mA, 100 MHz Current Feedback Amplifier
LM6182 - Dual 100 mA Output, 100 MHz Current Feedback Amplifier
LM6313 - High Speed, High Power Operational Amplifier
LM675 - Power Operational Amplifier
LM7171 - Very High Speed, High Output Current, Voltage Feedback Amplifier
GO
QUICK SEARCH
PARAMETRIC SEARCH
SYSTEM DIAGRAMS
PRODUCT TREE
HOME
Enter Word or
Feedback
Use of "Cookies"

FIG. 16

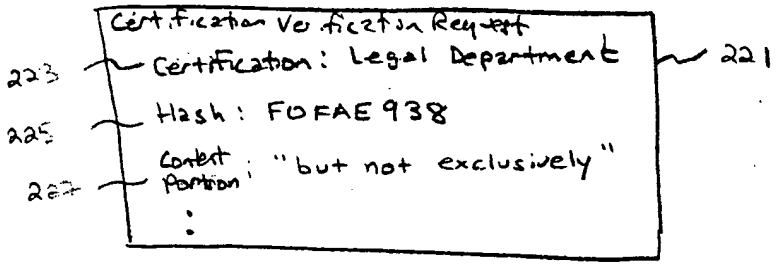

Certification Verification Request
223
Certification: Legal Department
221
225
Hash: F0FAE938
227
Content Portion: "but not exclusively"

FIG. 17

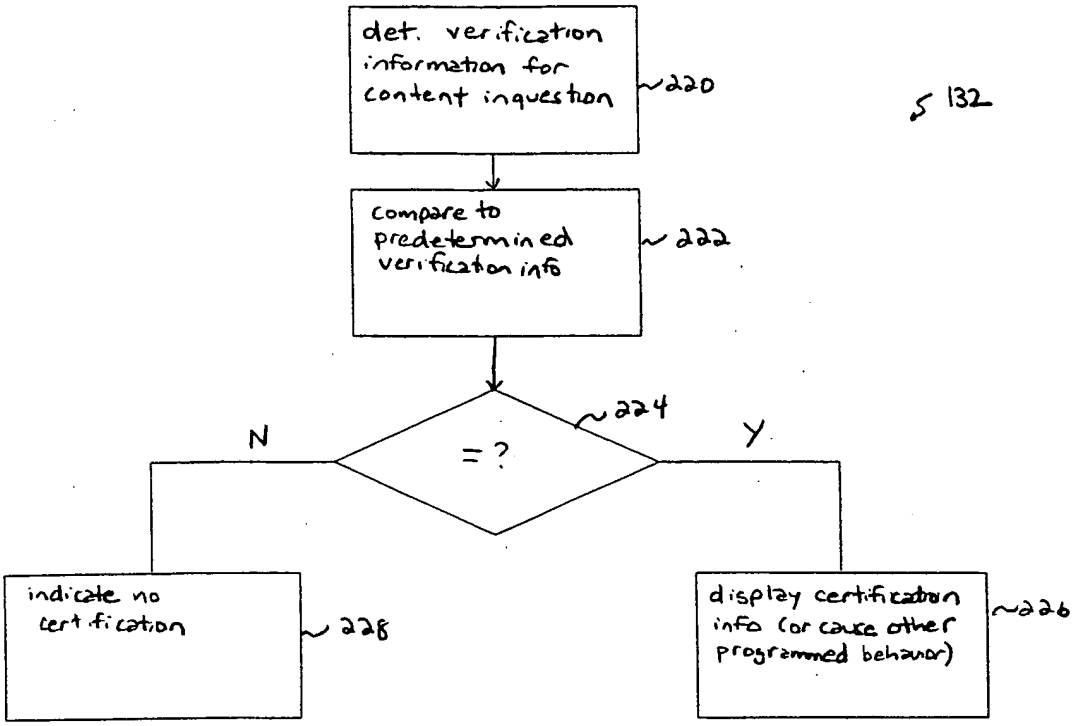

det. verification information for content inquestion
220
132
compare to predetermined verification info
222
224
=?
N
Y
indicate no certification
228
display certification info (or cause other programmed behavior)
226

FIG. 18

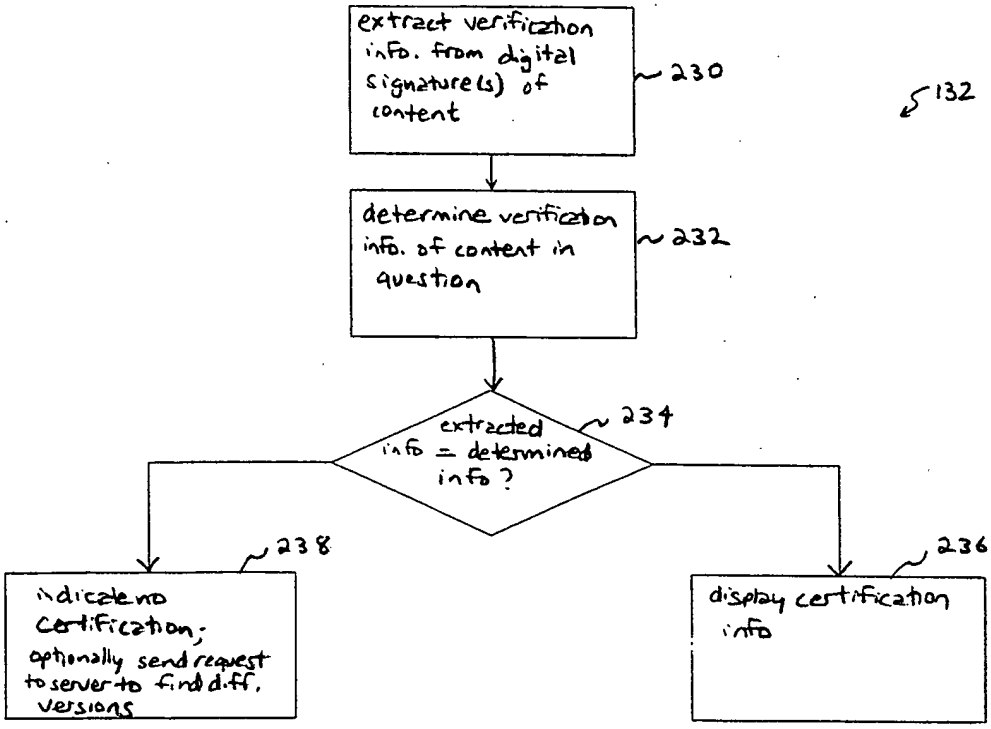

extract verification info. from digital signature(s) of content
230
132
determine verification info. of content in question
232
extracted info = determined info ?
234
indicate no certification; optionally send request to server to find diff. versions
238
display certification info
236

FIG. 19

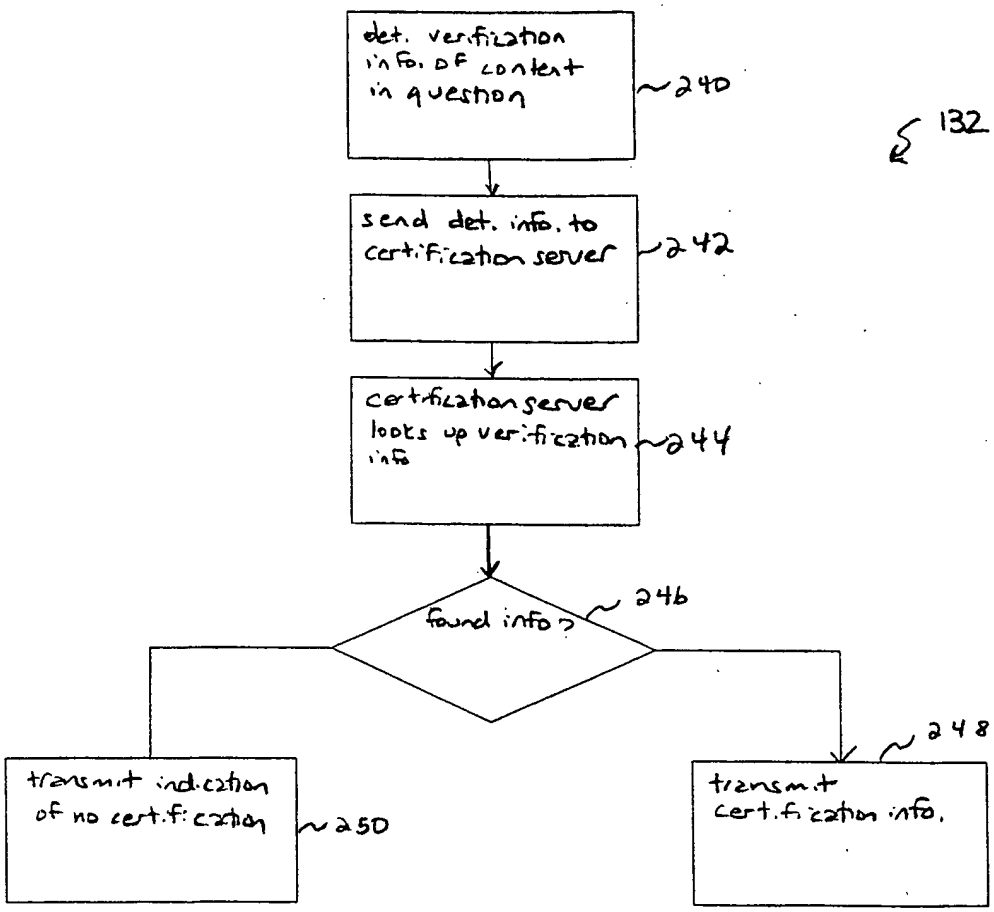

det. verification info. of content in question
240
132
send det. info. to certification server
242
certification server looks up verification info
244
found info?
246
transmit indication of no certification
250
transmit certification info.
248

FIG. 2D

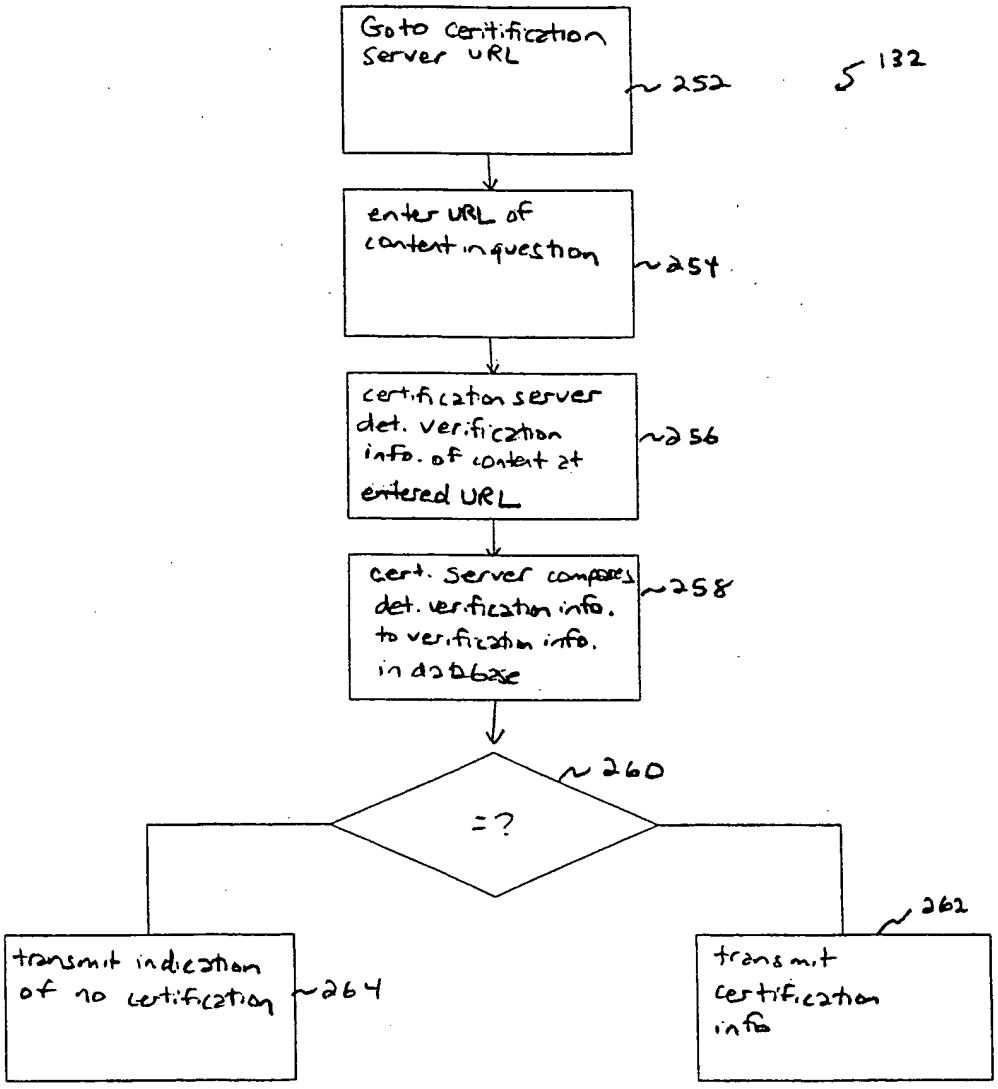

Go to certification server URL
252
132
enter URL of content in question
254
certification server det. verification info. of content at entered URL
256
cert. server compares det. verification info. to verification info. in database
258
260
=?
transmit indication of no certification
264
transmit certification info
262

FIG. 21

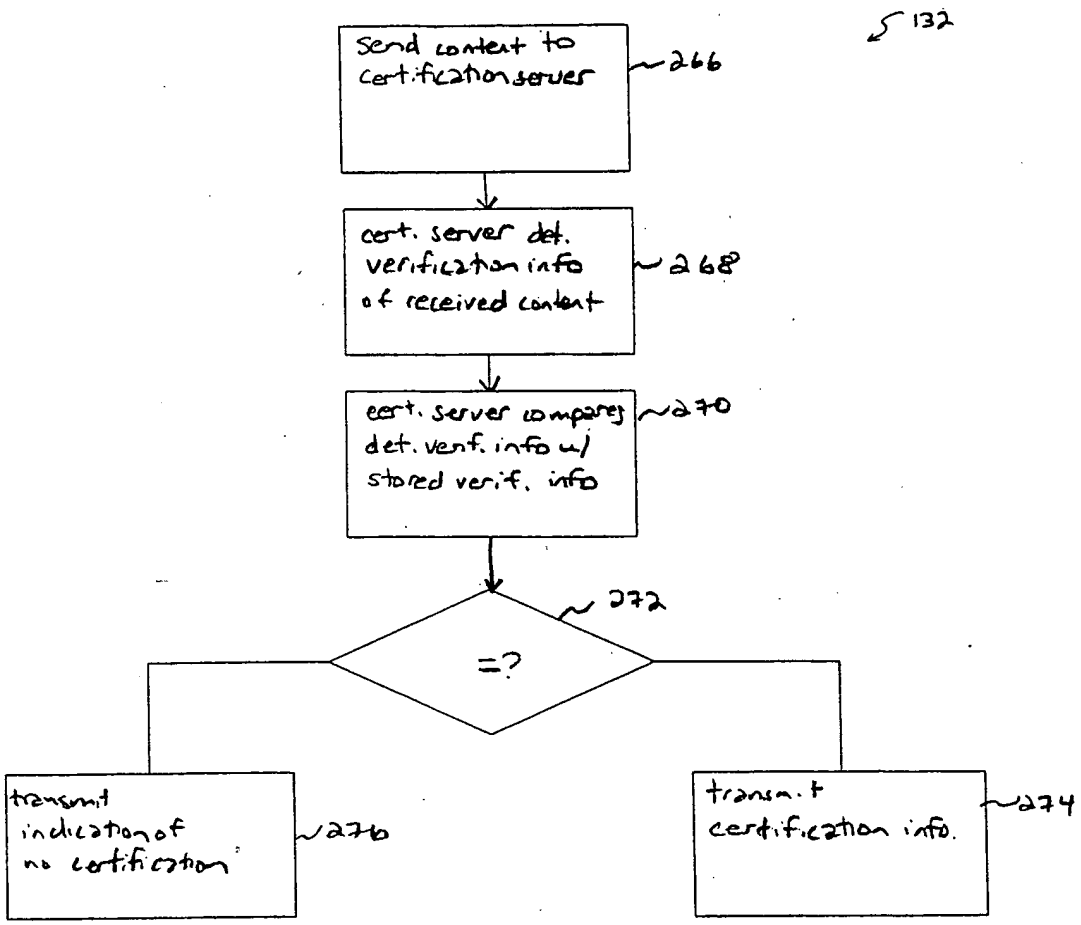

132
Send content to certification server
266
cert. server det. verification info of received content
268
cert. server compares det. verif. info w/ stored verif. info
270
272
=?
transmit indication of no certification
276
transmit certification info.
274

FIG. 22

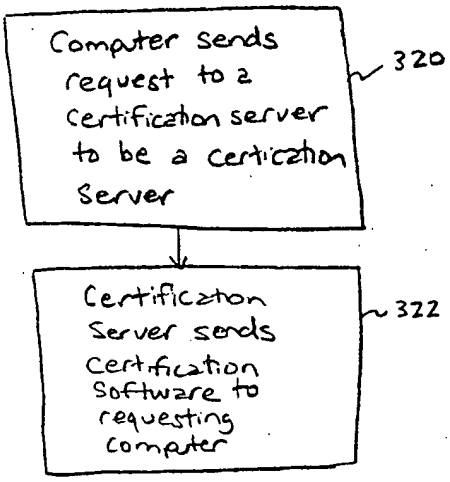

Computer sends request to a certification server to be a certication Server
320
Certification Server sends certification software to requesting computer
322

FIG. 23

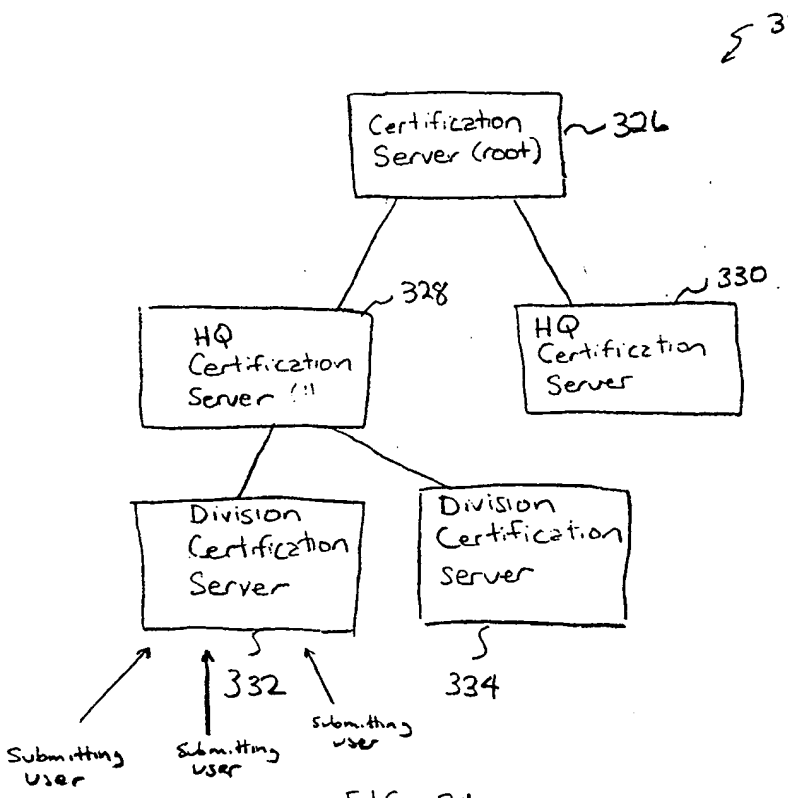

324
Certification Server (root)
326
328
330
HQ Certification Server
HQ Certification Server
Division Certification Server
Division Certification Server
332
334
Submitting User
Submitting User
Submitting User

FIG. 24

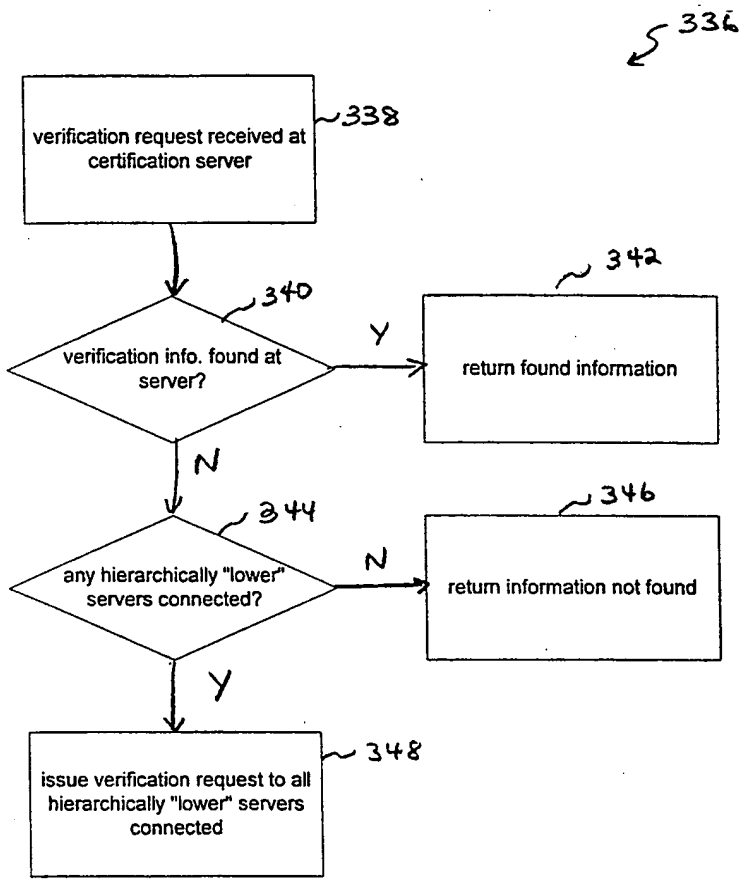

336
verification request received at certification server
338
verification info. found at server?
340
Y
return found information
342
N
any hierarchically "lower" servers connected?
344
N
return information not found
346
Y
issue verification request to all hierarchically "lower" servers connected
348

FIG. 25

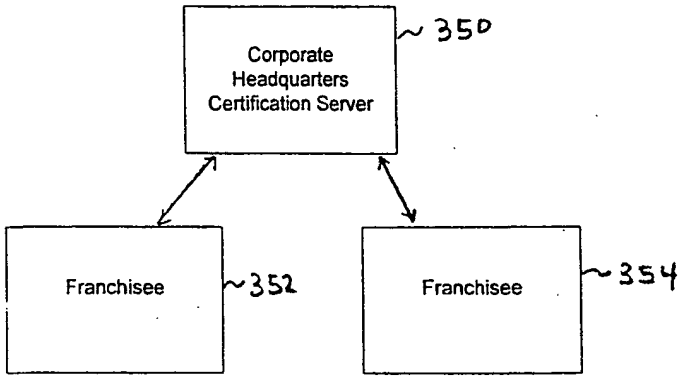

Corporate Headquarters Certification Server
350
Franchisee
352
Franchisee
354

FIG. 26

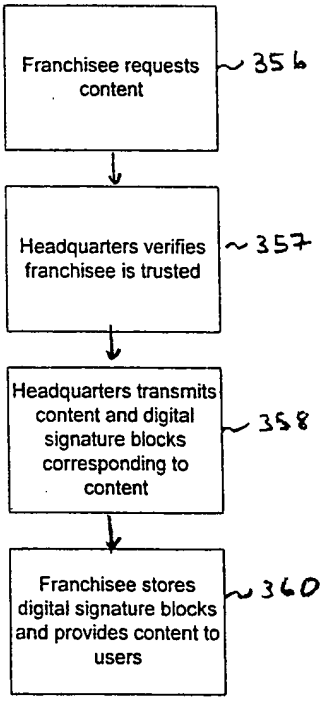

Franchisee requests content
356
Headquarters verifies franchisee is trusted
357
Headquarters transmits content and digital signature blocks corresponding to content
358
Franchisee stores digital signature blocks and provides content to users
360

FIG. 27

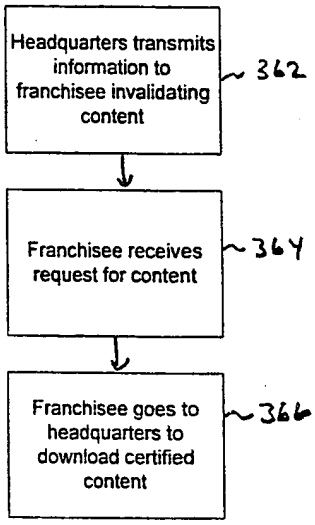

Headquarters transmits information to franchisee invalidating content
362
Franchisee receives request for content
364
Franchisee goes to headquarters to download certified content
366

FIG. 2B

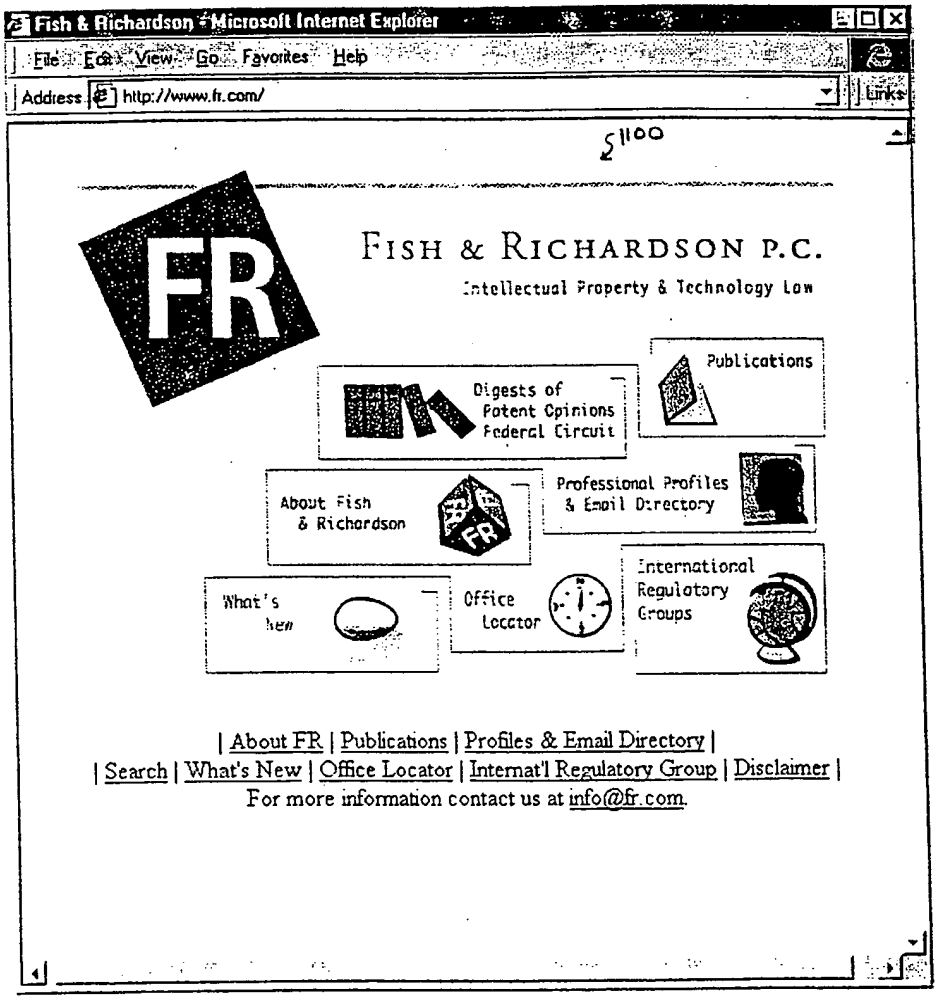

Fish & Richardson - Microsoft Internet Explorer
File Edit View Go Favorites Help
Address http://www.fr.com/
Links
1100
FISH & RICHARDSON P.C.
Intellectual Property & Technology Law
Publications
Digests of Patent Opinions Federal Circuit
About Fish & Richardson
Professional Profiles & Email Directory
What's New
Office Locator
International Regulatory Groups
| About FR | Publications | Profiles & Email Directory |
| Search | What's New | Office Locator | Internat'l Regulatory Group | Disclaimer |
For more information contact us at info@fr.com.

FIG. 29

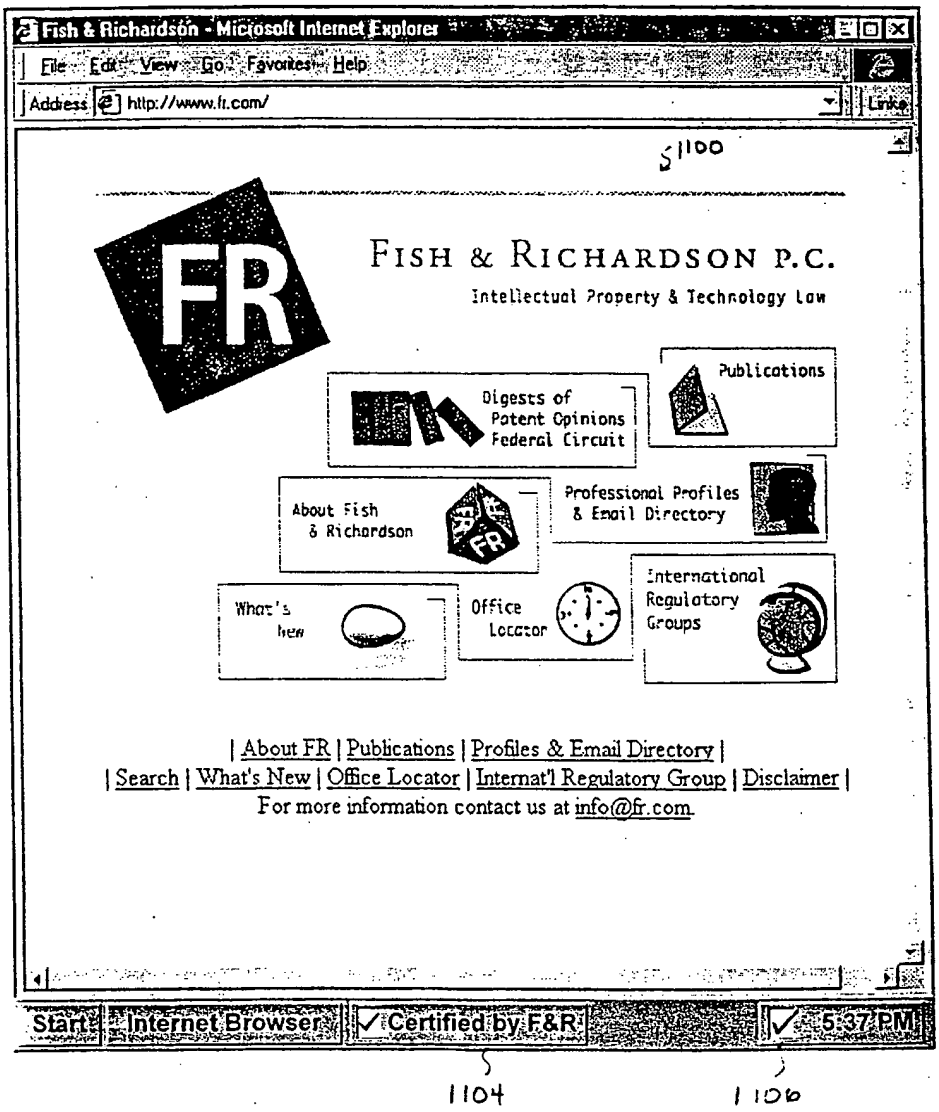

Fish & Richardson - Microsoft Internet Explorer
File Edit View Go Favorites Help
Address http://www.fr.com/
Links
1100
FISH & RICHARDSON P.C.
Intellectual Property & Technology Law
Digests of Patent Opinions Federal Circuit
Publications
About Fish & Richardson
Professional Profiles & Email Directory
What's New
Office Locator
International Regulatory Groups
| About FR | Publications | Profiles & Email Directory |
| Search | What's New | Office Locator | Internat'l Regulatory Group | Disclaimer |
For more information contact us at info@fr.com.
Start
Internet Browser
Certified by F&R
5:37 PM
1104
1106

FIG. 30

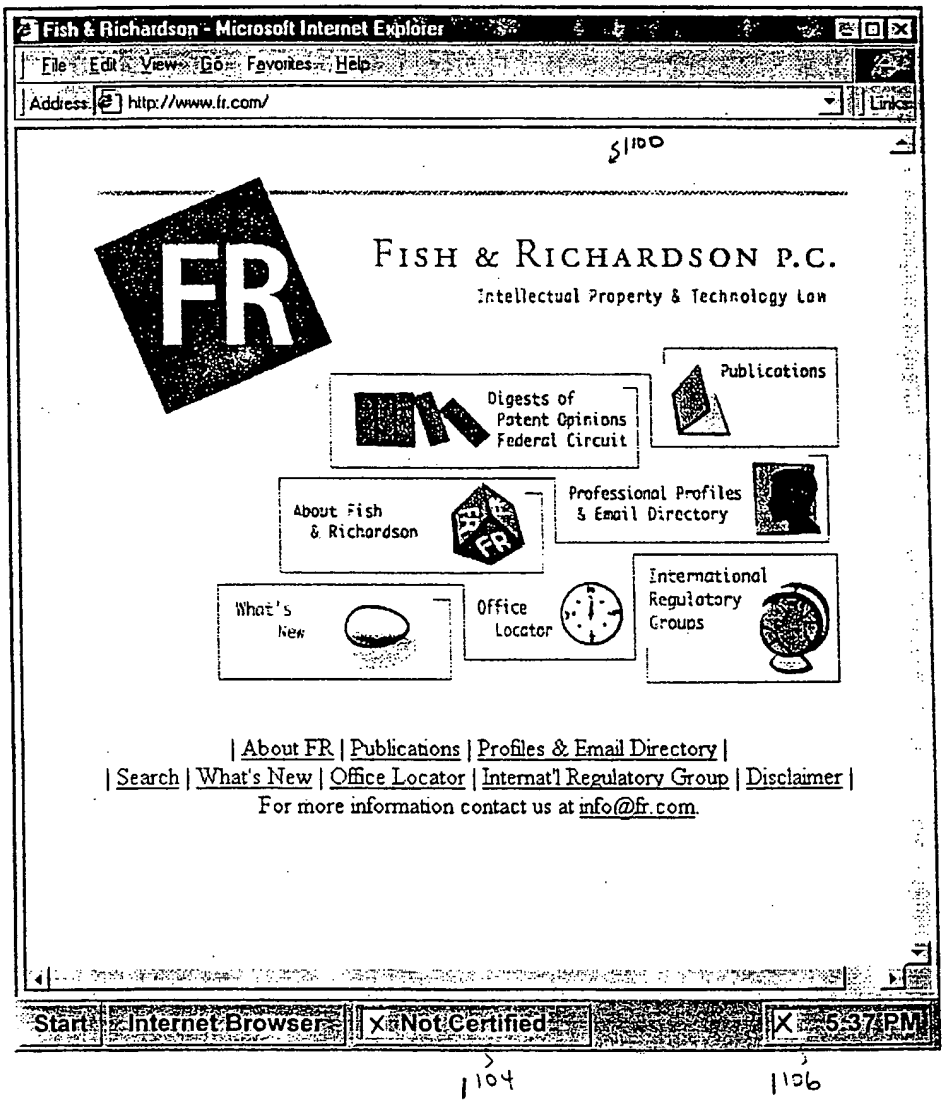

Fish & Richardson - Microsoft Internet Explorer
File Edit View Go Favorites Help
Address http://www.fr.com/
Links
1100
FISH & RICHARDSON P.C.
Intellectual Property & Technology Law
Publications
Digests of Patent Opinions Federal Circuit
About Fish & Richardson
Professional Profiles & Email Directory
What's New
Office Locator
International Regulatory Groups
| About FR | Publications | Profiles & Email Directory |
| Search | What's New | Office Locator | Internat'l Regulatory Group | Disclaimer |
For more information contact us at info@fr.com.
Start
Internet Browser
Not Certified
5:37 PM
1104
1106

FIG. 31

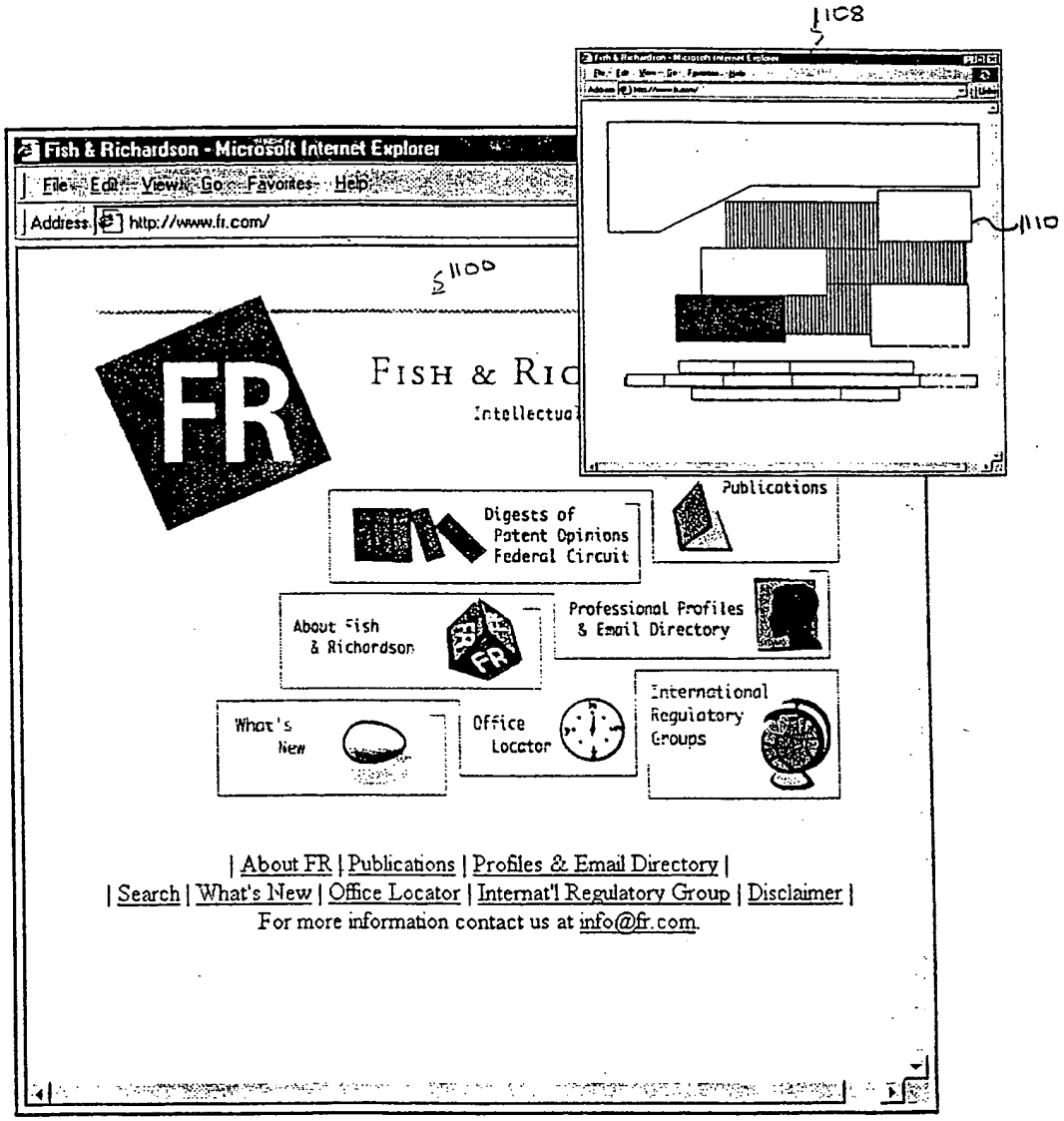

1108
1110
1100
Fish & Richardson - Microsoft Internet Explorer
File Edit View Go Favorites Help
Address http://www.fr.com/
FISH & RIC
Intellectua
Digests of Patent Opinions Federal Circuit
Publications
About Fish & Richardson
Professional Profiles & Email Directory
What's New
Office Locator
International Regulatory Groups
| About FR | Publications | Profiles & Email Directory |
| Search | What's New | Office Locator | Internat'l Regulatory Group | Disclaimer |
For more information contact us at info@fr.com.

FIG. 32

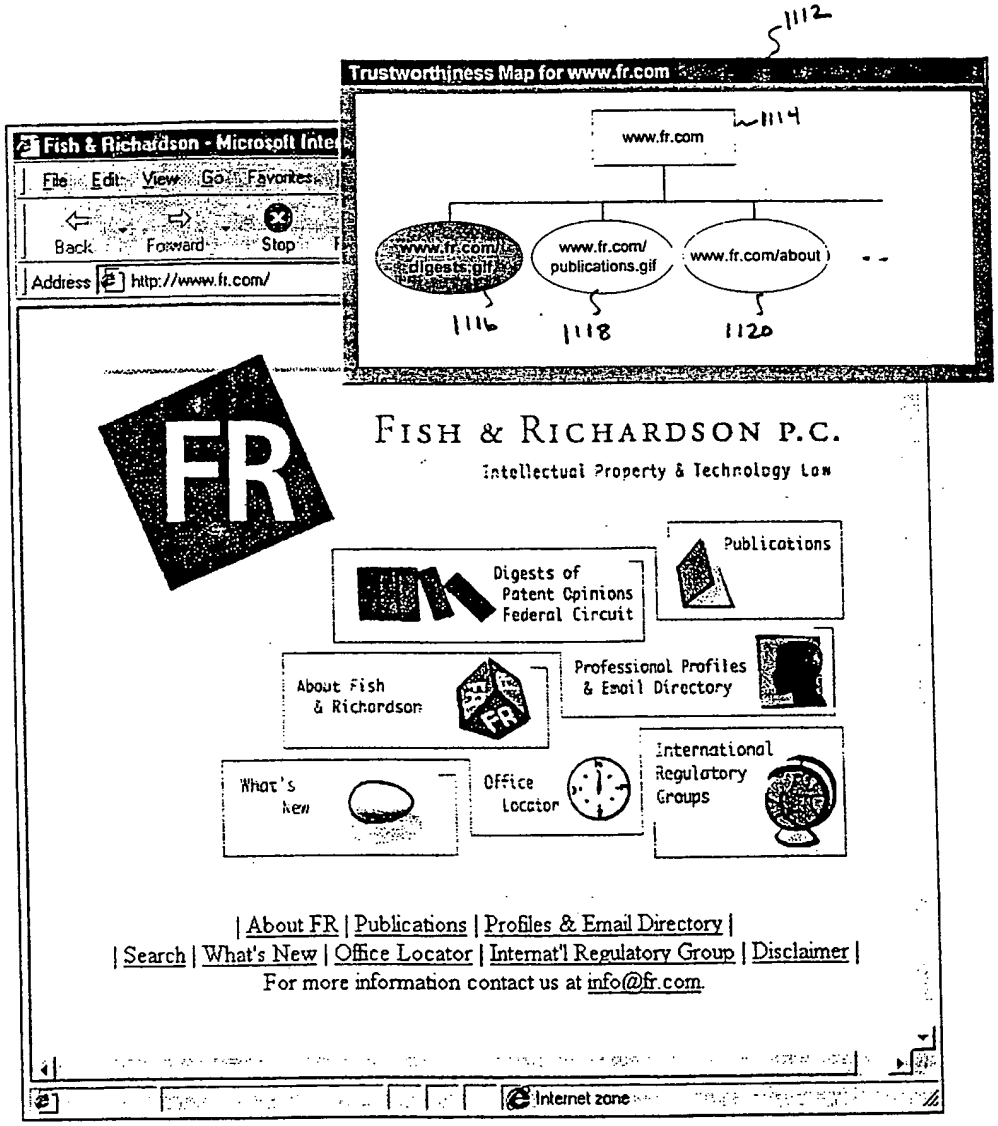

1112
Trustworthiness Map for www.fr.com
www.fr.com
1114
www.fr.com/ digests.gif
www.fr.com/ publications.gif
www.fr.com/about
1116
1118
1120
Fish & Richardson - Microsoft Inte
File Edit View Go Favorites
Back Forward Stop
Address http://www.fr.com/
FISH & RICHARDSON P.C.
Intellectual Property & Technology Law
Digests of Patent Opinions Federal Circuit
Publications
About Fish & Richardson
Professional Profiles & Email Directory
What's New
Office Locator
International Regulatory Groups
| About FR | Publications | Profiles & Email Directory |
| Search | What's New | Office Locator | Internat'l Regulatory Group | Disclaimer |
For more information contact us at info@fr.com.
Internet zone

FIG. 33

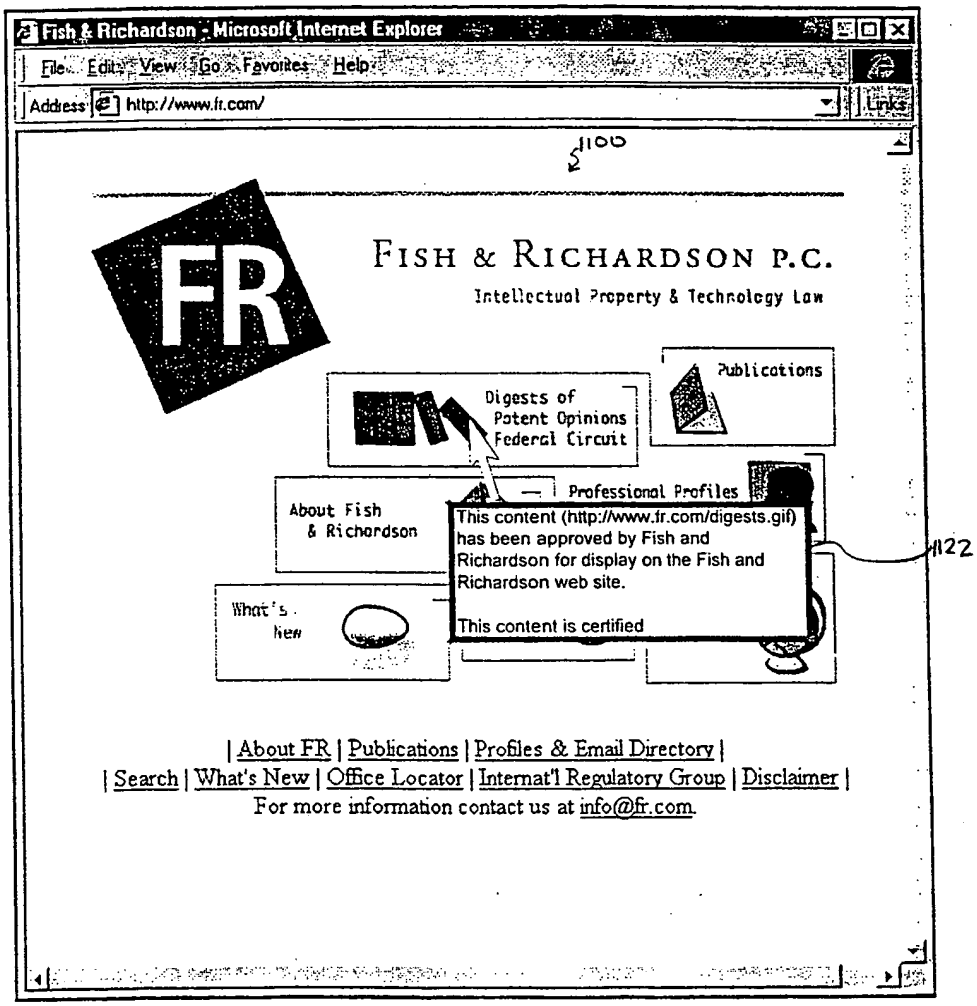

Fish & Richardson - Microsoft Internet Explorer
File Edit View Go Favorites Help
Address http://www.fr.com/
Links
1100
FISH & RICHARDSON P.C.
Intellectual Property & Technology Law
Publications
Digests of Patent Opinions Federal Circuit
Professional Profiles
About Fish & Richardson
What's New
This content (http://www.fr.com/digests.gif) has been approved by Fish and Richardson for display on the Fish and Richardson web site.
This content is certified
1122
| About FR | Publications | Profiles & Email Directory |
| Search | What's New | Office Locator | Internat'l Regulatory Group | Disclaimer |
For more information contact us at info@fr.com.

FIG. 34

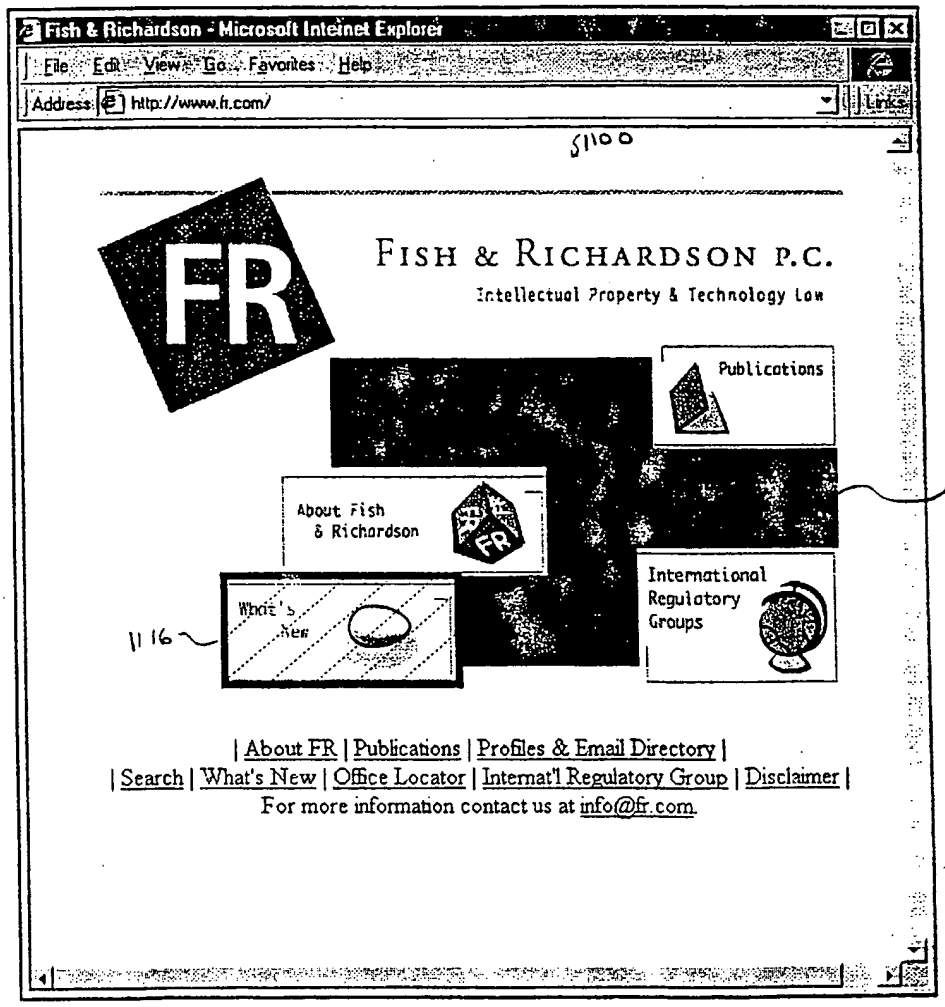

Fish & Richardson - Microsoft Internet Explorer
File Edit View Go Favorites Help
Address http://www.fr.com/
Links
1100
FISH & RICHARDSON P.C.
Intellectual Property & Technology Law
Publications
About Fish & Richardson
International Regulatory Groups
What's New
1114
1116
| About FR | Publications | Profiles & Email Directory |
| Search | What's New | Office Locator | Internat'l Regulatory Group | Disclaimer |
For more information contact us at info@fr.com.

FIG. 35

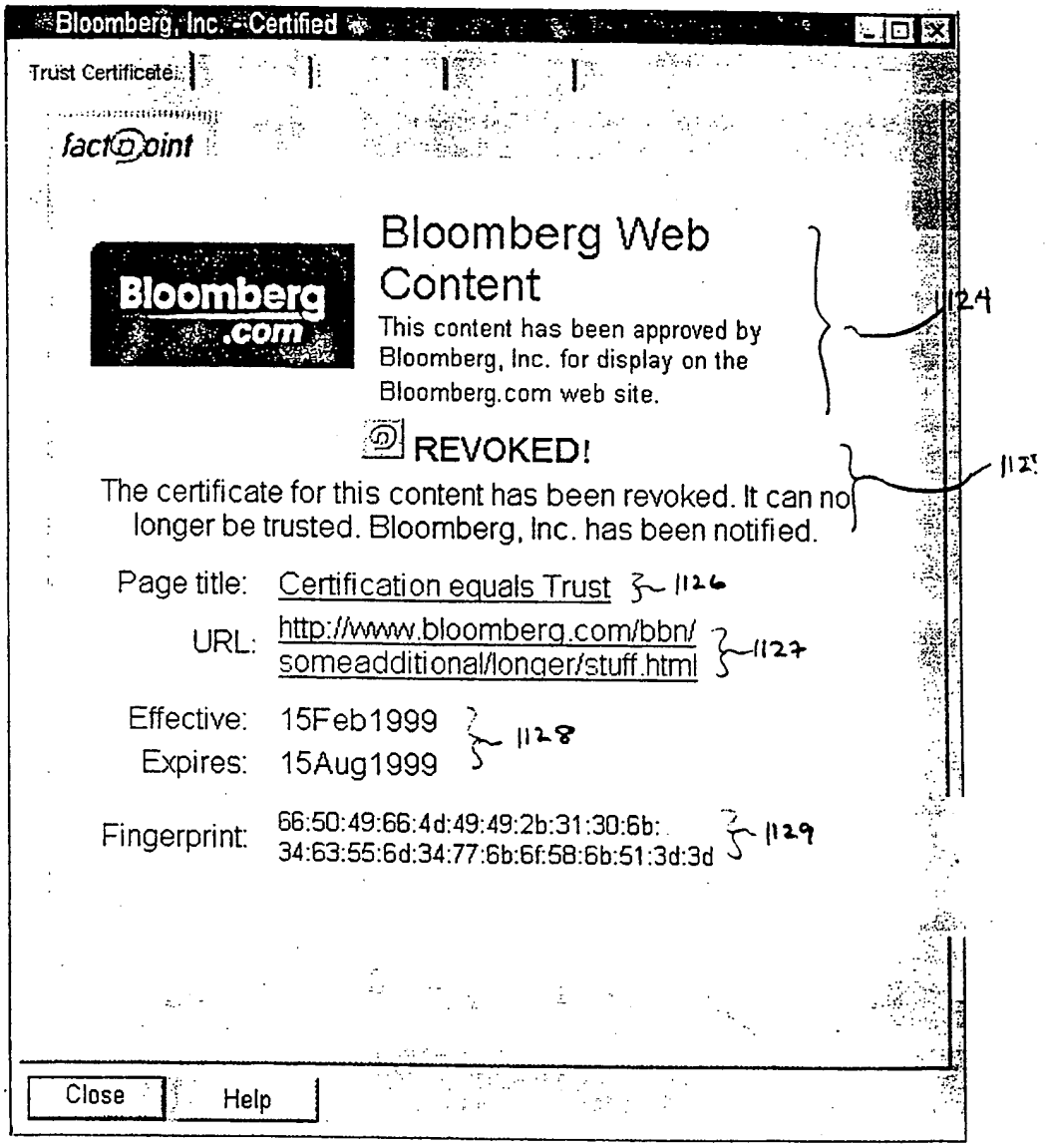

Bloomberg, Inc. - Certified
Trust Certificate:
factpoint
Bloomberg .com
Bloomberg Web Content
This content has been approved by Bloomberg, Inc. for display on the Bloomberg.com web site.
1124
REVOKED!
The certificate for this content has been revoked. It can no longer be trusted. Bloomberg, Inc. has been notified.
1125
Page title: Certification equals Trust
1126
URL: http://www.bloomberg.com/bbn/someadditional/longer/stuff.html
1127
Effective: 15Feb1999
Expires: 15Aug1999
1128
Fingerprint: 66:50:49:66:4d:49:49:2b:31:30:6b:34:63:55:6d:34:77:6b:6f:58:6b:51:3d:3d
1129
Close
Help

FIG. 36

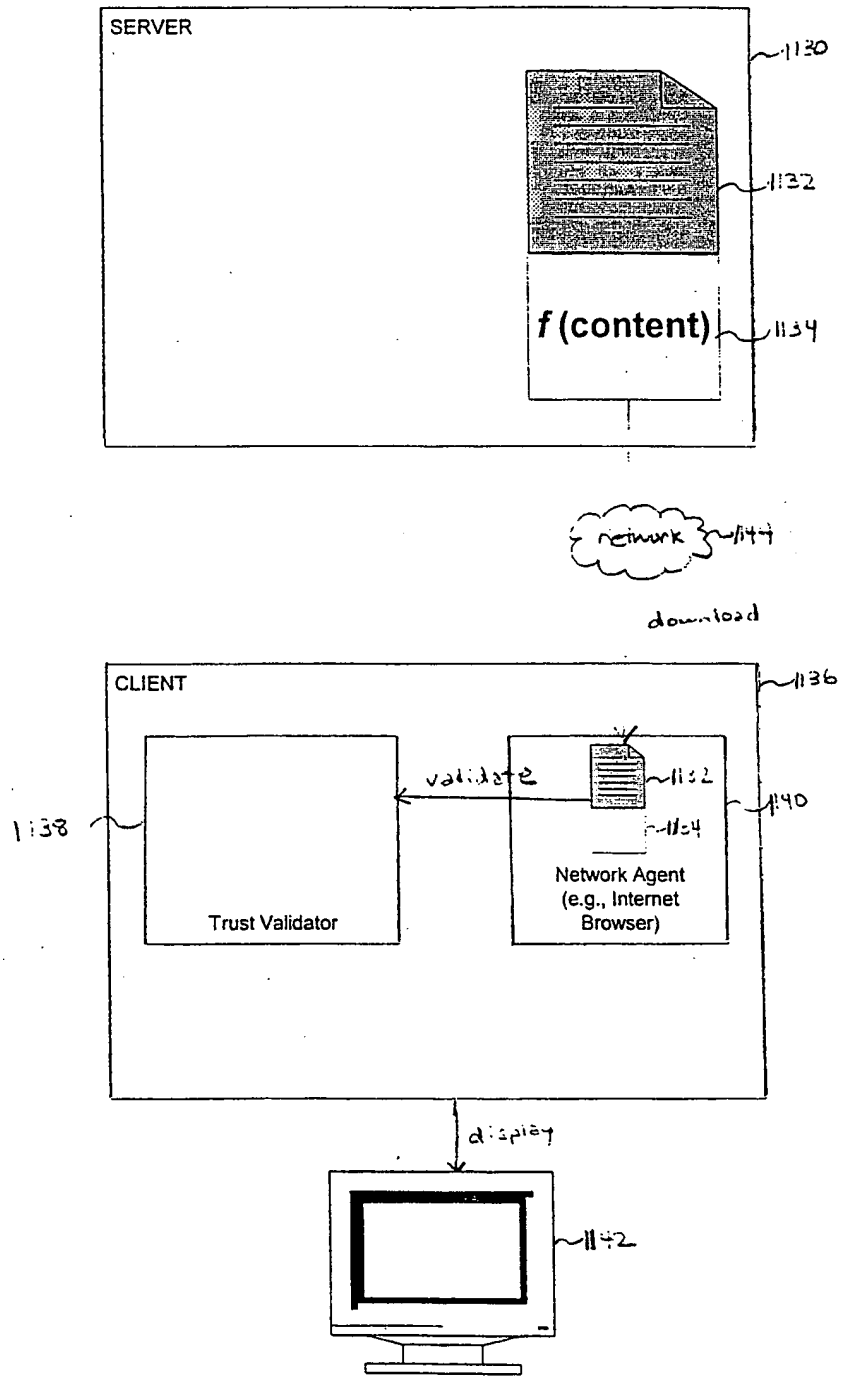

SERVER
1130
1132
f (content)
1134
network
1144
download
CLIENT
1136
validate
1132
1140
1134
1138
Trust Validator
Network Agent
(e.g., Internet
Browser)
display
1142

FIG 37

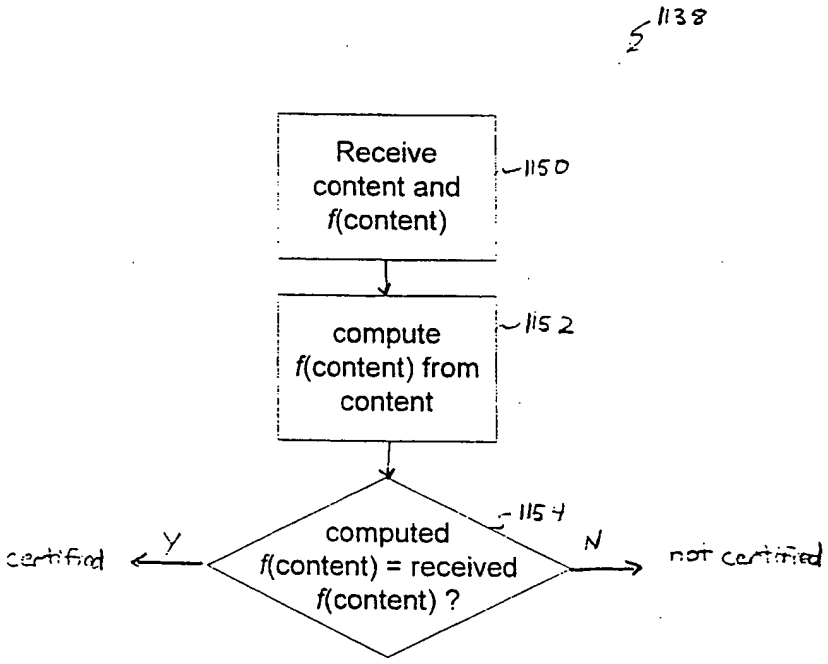

1138
Receive content and f(content)
1150
compute f(content) from content
1152
computed f(content) = received f(content) ?
1154
Y
certified
N
not certified

FIG. 38

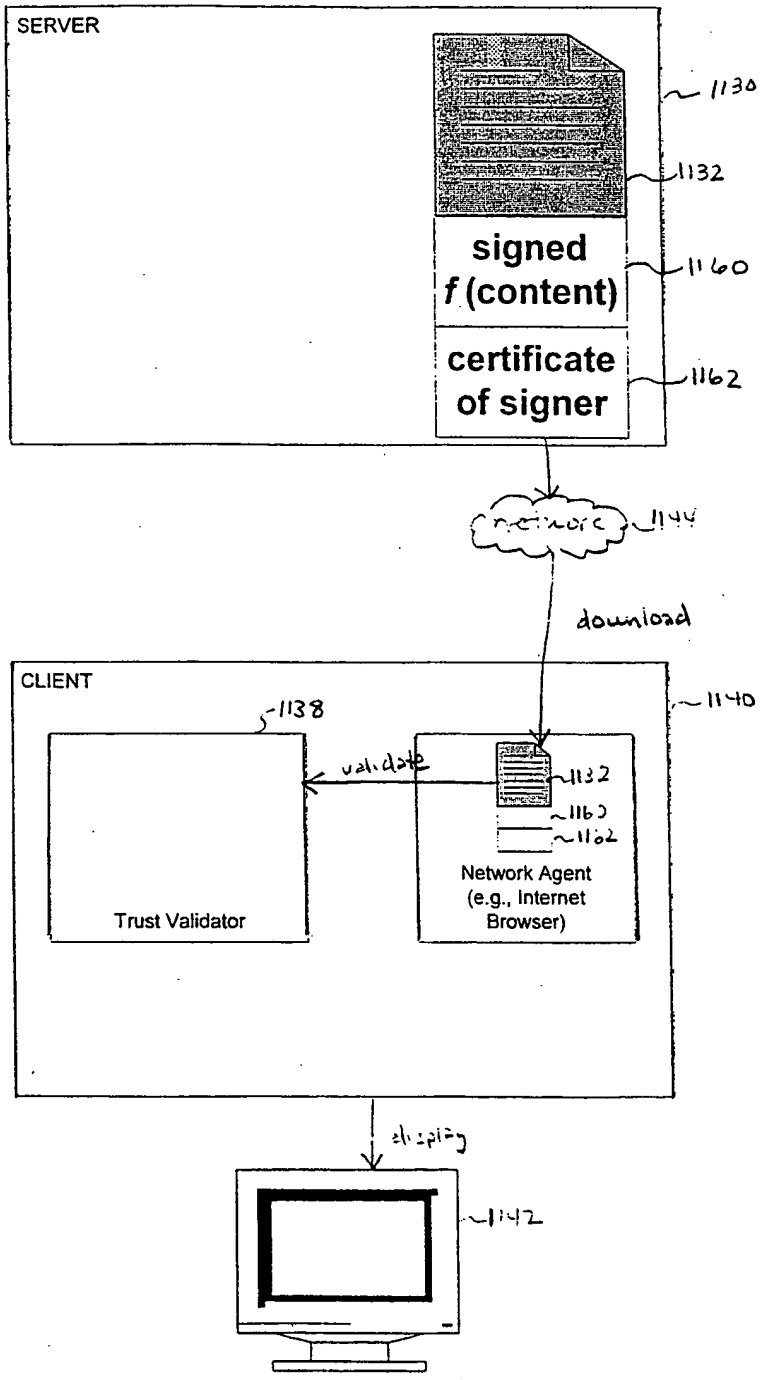

SERVER
1130
1132
signed
f (content)
1160
certificate
of signer
1162
network
1144
download
CLIENT
1140
1138
validate
1132
1160
1162
Trust Validator
Network Agent
(e.g., Internet
Browser)
display
1142

FIG. 39

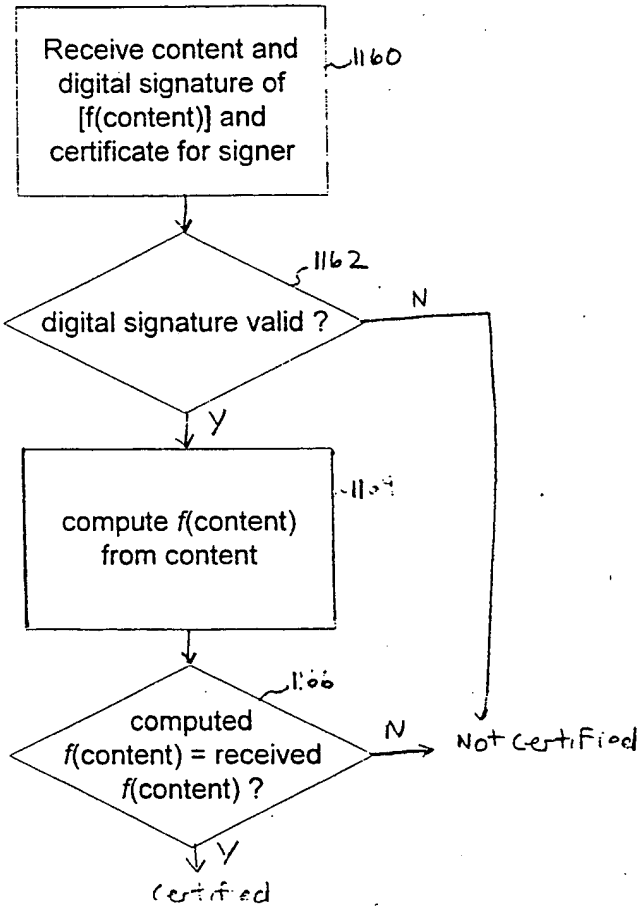

Receive content and digital signature of [f(content)] and certificate for signer
1160
1162
digital signature valid ?
N
Y
compute f(content) from content
1164
1166
computed f(content) = received f(content) ?
N
Not Certified
Y
Certified

FIG. 40.

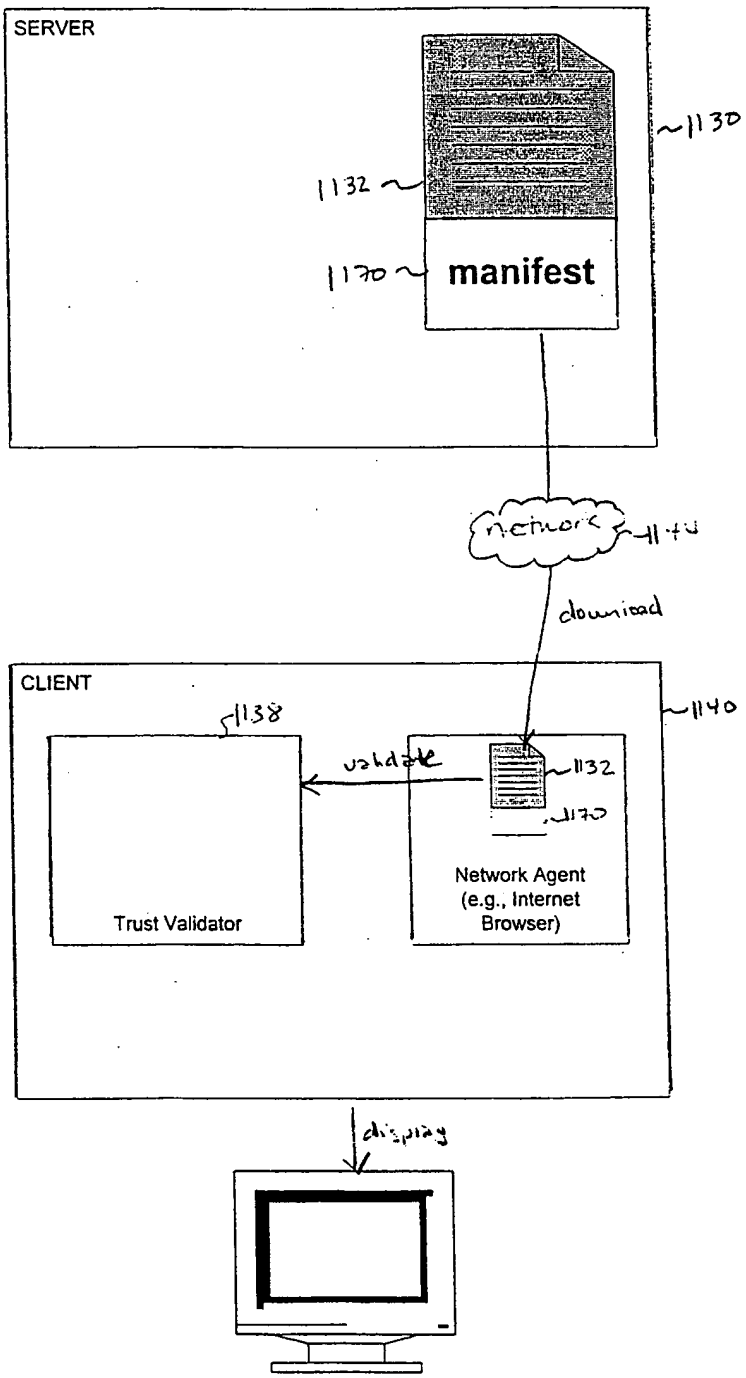

SERVER
1130
1132
1170
manifest
network
1140
download
CLIENT
1140
1138
validate
1132
1170
Trust Validator
Network Agent
(e.g., Internet
Browser)
display

FIG. 41

1170

Contents	f (content)
www.fr.com	984emf9
www.fr.com/digests.gif	29482jd9
www.fr.com/publications.gif	2930843f
www.fr.com/about.gif	23901233
.	
.	

FIG. 42

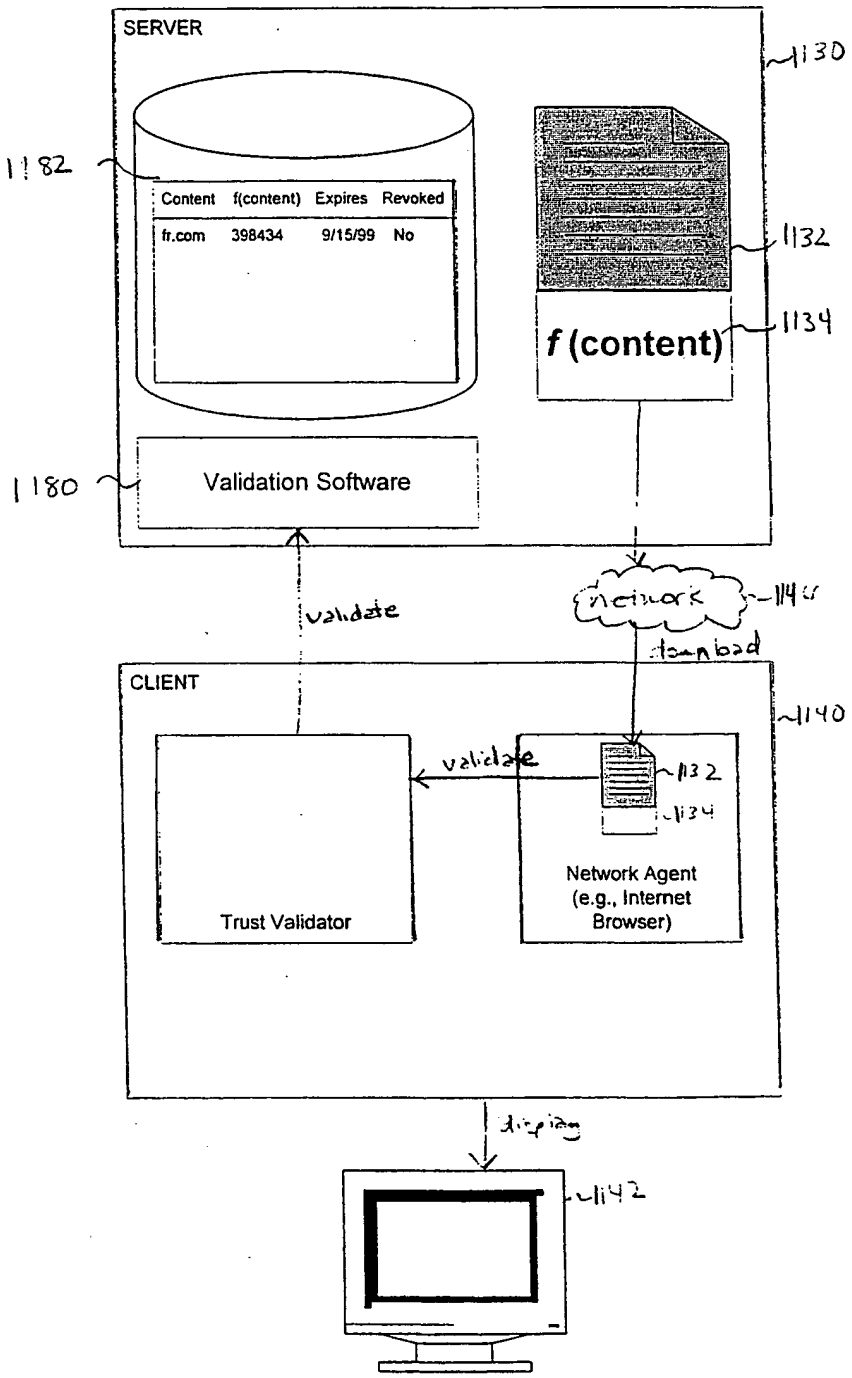

SERVER
1130
1182
Content f(content) Expires Revoked
fr.com 398434 9/15/99 No
1132
f (content)
1134
1180
Validation Software
validate
network
1140
CLIENT
validate
1132
1134
Trust Validator
Network Agent
(e.g., Internet
Browser)
1142

FIG. 43

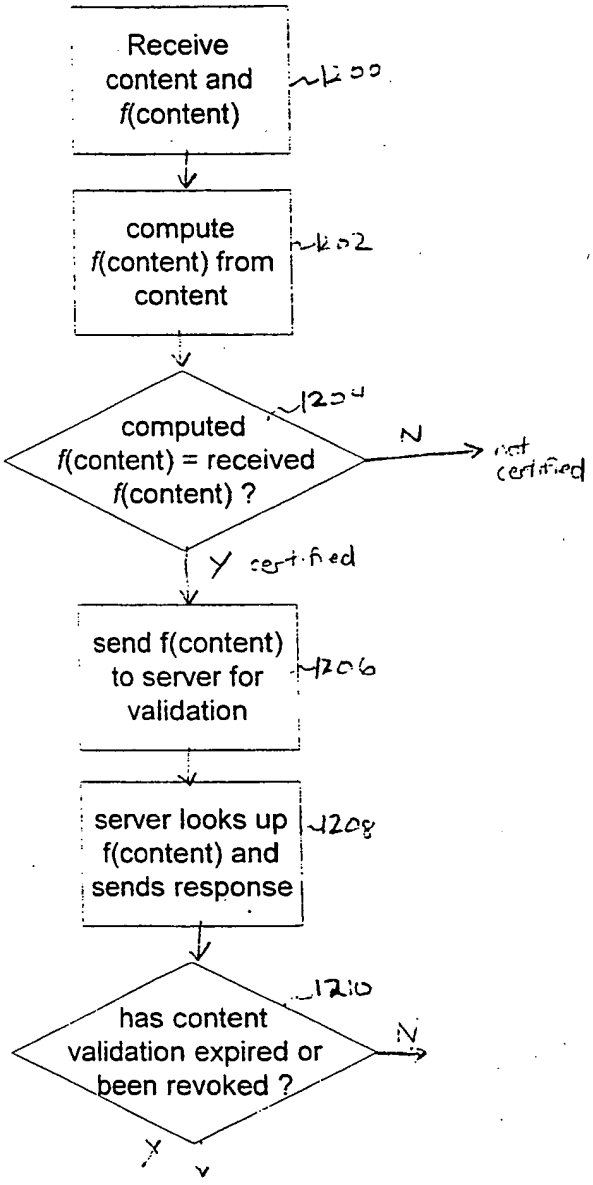

Receive content and f(content)
1200
compute f(content) from content
1202
computed f(content) = received f(content) ?
1204
N
not certified
Y certified
send f(content) to server for validation
1206
server looks up f(content) and sends response
1208
has content validation expired or been revoked ?
1210
N
Y

FIG. 44

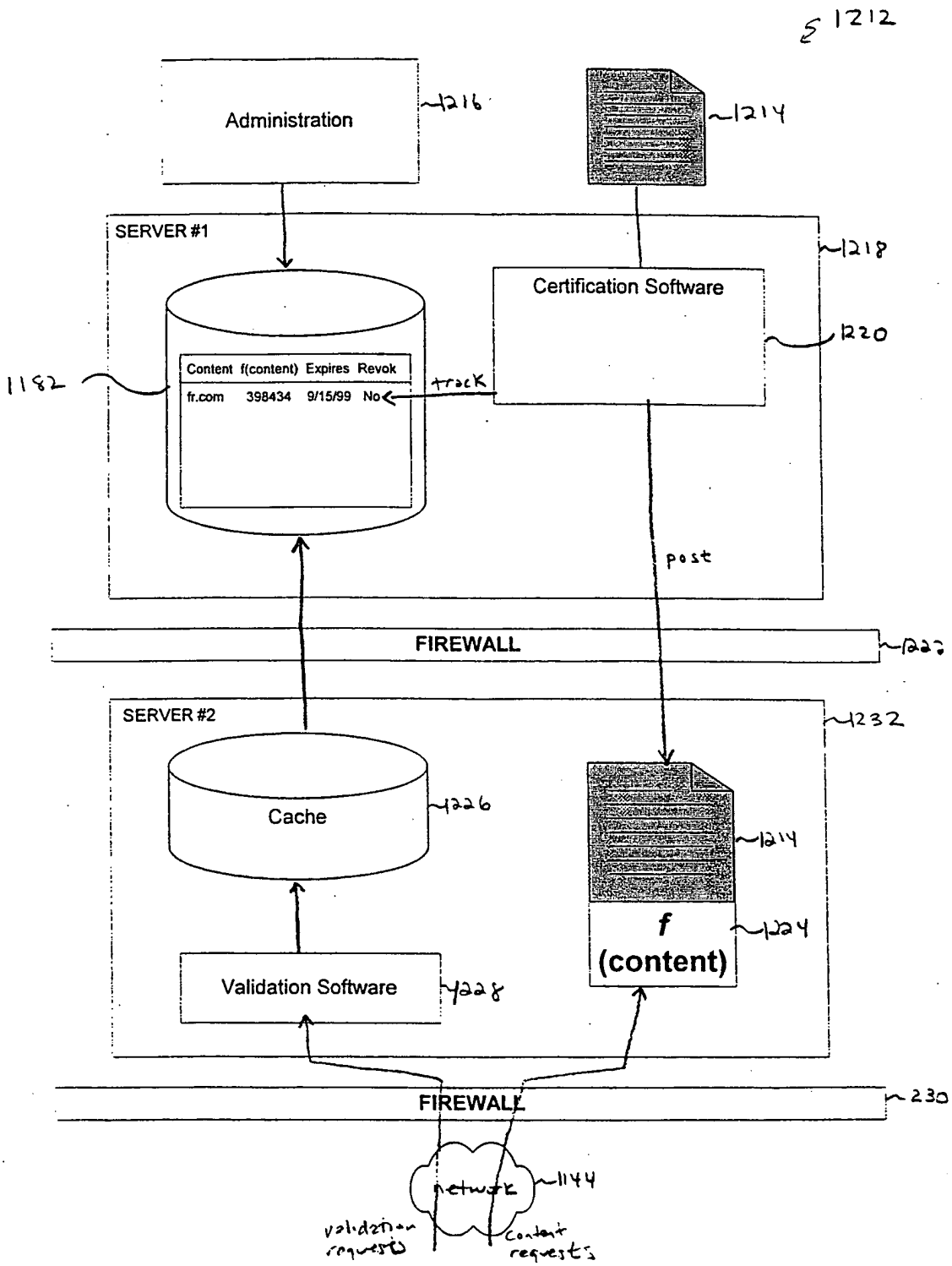

1212
Administration
1216
1214
SERVER #1
1218
Certification Software
1220
Content f(content) Expires Revok
fr.com 398434 9/15/99 No
1182
track
post
FIREWALL
1222
SERVER #2
1232
Cache
1226
1214
f
(content)
1224
Validation Software
1228
FIREWALL
1230
network
1144
validation requests
content requests

FIG. 45

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/03489

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) :G06F 13/00
US CL :709/200; 705/44; 713/201
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 709/200; 705/44; 713/201

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A,T	US 6,058,383 A (NARASIMHALU ET AL) 02 MAY 2000, ALL	1-42
A,T	US 6,026,166 A (lEBOURGEOIS) 15 FEBRUARY 2000, ALL	1-42
A,P	US 5,903,882 A (ASAY ET AL) 11 MAY 1999, ALL	1-42
A,P	US 6,018,724 A (ARENT) 25 JANUARY 2000, ALL	1-42

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search	Date of mailing of the international search report
27 JUNE 2000	19 JUL 2000
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer GLENTON BURGESS Telephone No. (703) 305-4792

Form PCT/ISA/210 (second sheet) (July 1998) *

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

CORRECTED VERSION

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 August 2000 (10.08.2000)

PCT

(10) International Publication Number
WO 00/46681 A1

(51) International Patent Classification[7]: G06F 13/00

(21) International Application Number: PCT/US00/03489

(22) International Filing Date: 8 February 2000 (08.02.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

09/248,370	8 February 1999 (08.02.1999)	US
60/153,901	14 September 1999 (14.09.1999)	US

(63) Related by continuation (CON) or continuation-in-part (CIP) to earlier applications:

US	09/248,370 (CIP)
Filed on	8 February 1999 (08.02.1999)
US	60/153,901 (CIP)
Filed on	14 September 1999 (14.09.1999)

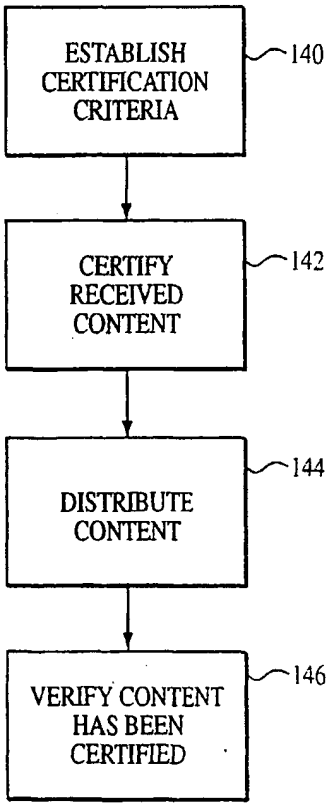
(71) Applicant *(for all designated States except US)*: **GEOTRUST, INC.** [US/US]; Suite 20, 40 Washington Street, Wellesley Hills, MA 02481 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **COULTHARD, Christopher, M.** [GB/US]; 88 Park Avenue #402, Arlington, MA 02476 (US). **MCLEOD, Scott, C.** [US/US]; 24 Carriage Drive, Chelmsford, MA 01824 (US). **NORMAN, Peter, D.** [US/US]; 56 Palmer Street, Arlington, MA 02174 (US). **WILLOUGHBY, Kevin** [US/US]; 10 Church Street, Framingham, MA 01702 (US). **HODGMAN, Rod, G.** [US/US]; 465 Robinson Road, Boxborough, MA 01719

[Continued on next page]

(54) Title: CONTENT CERTIFICATION



(57) Abstract: A method of processing content includes storing verification information corresponding to certified content at a first computer (140) and receiving a verification request corresponding to content from a second computer (142). The method also includes determining a verification information for the content corresponding to the verification request and comparing the determined verification information with the stored verification information (146).

WO 00/46681 A1

(US). **ROSENBERG, Jonathan** [—/US]; 11 Seton Hill Road, Auburndale, MA 02466 (US).

(74) **Agents: LEE, G., Roger** et al.; Fish & Richardson P.C., 225 Franklin Street, Boston, MA 02110-2804 (US).

(81) **Designated States** *(national)*: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) **Designated States** *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

(48) **Date of publication of this corrected version:**
20 September 2001

(15) **Information about Correction:**
see PCT Gazette No. 38/2001 of 20 September 2001, Section II

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

CONTENT CERTIFICATION

Reference to Related Applications

This application relates to pending U.S. application Serial No. 09/248,370, entitled "Content Certification", filed on February 8, 1999 and U.S. Provisional Application Number 60/153,901 filed September 14, 1999. These applications are incorporated by reference in their entirety herein.

Background of the Invention

The Internet and the World Wide Web have made information dissemination fast, easy, and cheap. Postings from both businesses and individuals have contributed to the wealth of available information. Unfortunately, the available information is sometimes of dubious value. For example, in 1998 a news agency accidentally posted a pre-written obituary of Bob Hope on its Web-site. Congress held a moment of silence in his honor. The report of Mr. Hope's demise, however, was greatly exaggerated. Other Internet postings have been less innocuous such as the accidental pre-release of economic data by the U.S. Bureau of Labor and Statistics.

In addition to accidental postings, some information available on the Internet, purporting to be from official sources, includes intentionally fabricated data or malicious statements. As a result, users tend to be somewhat skeptical of information accessed from the Internet. Additionally, some businesses, wary of potential liability or embarrassment, have begun to err on the side of safety and withhold information from Internet publication. These factors combine to reduce the effectiveness of the Internet as a communication medium.

Summary of the Invention

In general, in one aspect, a method of processing content includes storing verification information corresponding to certified content at a first computer and

receiving a verification request corresponding to content from a second computer. The method determines verification information for the content corresponding to the verification request and compares the determined verification information with the stored verification information.

Embodiments may include one or more of the following features. The method may feature receiving content certification criteria that can be used to determine whether content should be certified. The content certification criteria can be a list of required approval or programmed logic. The method may also feature storing certification information (e.g., a type of certification granted, entities approving certification, and when the content was certified). The verification information can include information derived from the content such as at least one hash key.

The verification request can include a URL. This can enable determination of verification information by collecting content from the URL included in the verification request.

The verification request can include content. This can enable determination of verification information by determining verification information for the content included in the verification request.

The verification request can include verification information. This can enable determination of verification information by merely using information included in the verification request.

Receiving a verification request may be produced by user interaction with a certification indicator, for example, a certification indicator included in the content.

The certification indicator can include a graphic image having associated instructions that produce a verification request. The method may further include transmitting certification information to the second computer.

The content may include graphics, text, animation, sound, and instructions. The content may form a web-page.

The comparing may include issuing verification requests to connected certification servers.

In general, in another aspect, a method includes presenting an indication that content is certified and receiving user input requesting certification verification of the content. The method further includes transmitting a certification verification request to a certification server and receiving information indicating whether the content has actually been certified.

Embodiments may include one or more of the following features. Presenting an indication may include presenting a user interface control. The method may further include displaying information included in the information received (e.g., content authorship, revision number, expiration date, and type of certification).

Transmitting a certification verification request may include transmitting verification information determined from the content such as one or more hash keys. Transmitting a certification verification request may include transmitting information included in the content.

Transmitting a certification verification may include transmitting a URL.

In general, in another aspect, a method of controlling content distribution includes receiving certification criteria for content to be distributed,

identifying content to be distributed, and determining whether the identified content satisfies the received certification criteria.

Embodiments may include one or more of the following features. Identifying content may include receiving a request for content at a server. Identifying content may include collecting content from a set of locations. Determining whether the content satisfies the certification criteria may include identifying at least one digital signature associated with the content and/or determining verification information (e.g., a hash key) for the content.

Advantages may include one or more of the following features. The techniques provide users with a simple and intuitive method of verifying that content (e.g., a web-page) has been certified by an organization. Verification can be a mouse-click away when content includes a certification indicator. Underlying mechanisms protect the verification process from falsification and tampering. These mechanisms enable users to trust the authenticity of displayed content.

The techniques also enable an organization to carefully define certification procedures that content must undergo before certification and distribution. Automating these certification procedures enables an organization to vigilantly control the quality and reliability of information provided.

Different implementation architectures permit distribution of certification functions across different computers and potentially speeding certification verification.

Other advantages of the invention will become apparent in view of the following description, including the figures, and the claims.

Brief Description of the Drawings

FIG. 1 is a screenshot of content that includes a certification indicator.

FIG. 2 is a screenshot of information that verifies content certification.

FIG. 3 is a flowchart of a process for certifying content.

FIG. 4 is a flow diagram of a certification and certification verification of content.

FIG. 5 is a flowchart of a certification procedure.

FIG. 6 is a block diagram of a certification scheme.

FIGS. 7A and 7B are screenshots of user interfaces for submitting content for certification.

FIG. 8 is a flow diagram of content certification.

FIG. 9 is a flowchart of content certification.

FIG. 10 is a diagram of information stored at a certification server.

FIG. 11 is a diagram of digital signature blocks issued for certified content.

FIG. 12 is a block diagram of a certification server and certified content.

FIGS. 13-14 are flowcharts of processes for monitoring posted content.

FIGS. 15-16 are screenshots of graphical user interfaces that include certification indicators.

FIG. 17 is a diagram of a certification verification request.

FIGS. 18-22 are flowcharts of processes for certification verification.

FIG. 23 is a flowchart of a process for creating multiple certification servers.

FIG. 24 is a block diagram of a hierarchy of certification servers.

FIG. 25 is a flowchart of a certification verification process using multiple certification servers.

FIG. 26 is a block diagram of franchisee certification servers.

FIG. 27 is a flowchart of a process for transmitting content to a franchisee server.

FIG. 28 is a flowchart of a process for updating content offered by a franchisee server.

FIG. 29 is a screenshot of a browser's display of an Internet page.

FIGS. 30-36 are screenshots of different persistent displays that notify a user whether content is certified.

FIGS. 37, 39, 41, and 43 are diagrams of systems for validating content certification.

FIGS. 38, 40, and 44 are flow-charts of processes for validating content certification.

FIG. 42 is a diagram of a manifest of web-page contents.

FIG. 45 is a diagram of a certification server and a validation server.

Description of the Preferred Embodiments

Introduction

Referring to FIG. 1, a browser's graphical user interface 100 (e.g., Netscape™ Navigator™) presents content 104 provided by a resource (e.g., a file) at a URL (Universal Resource Locator) 102. The content 104 can include graphics, text, animation, sound, instructions (e.g., Java Applets), etc. A URL 102 can refer to a location on a remote computer that stores the content 104 as data and presentation instructions. The presentation instructions and data can be in a variety of formats such as HTML (HyperText Markup Language), XML (Extensible Markup Language), PDF (Portable Document Format), JPEG (Joint Photographic Experts Group), and MPEG (Moving Picture Experts Group). When a browser requests content 104 from a URL 102 resource, a remote computer providing the resource can transmit the content 104 to a browser for presentation. As shown, the browser is an independent application, however, other applications (e.g., an e-mail program, a word processor, or a spread-sheet) can incorporate functions traditionally performed by the browser.

As shown in FIG. 1, the browser display 100 includes a certification indicator 106. The indicator 106 provides a simple method of ensuring that the

content 104 presented has undergone a certification process. Content 104 may include one or more certification indicators 106 (e.g., "Certified by the Legal Department" and "Certified by the Marketing Department"). As shown, the indicator 106 is a user interface control that has a graphic image, however, different implementations can present the control to a user as text, sounds, or by using other user interface techniques. User selection of the indicator 106 (e.g., using a mouse or other pointing device to click on the graphic image) initiates a certification verification process that can confirm that the content presented is the same content that has undergone the certification process claimed by the certification indicator 106.

Referring to FIG. 2, the certification verification process can produce a window 108 that includes a display of information describing the content's 104 certification such as the entities that have approved the content 114, when such approval occurred 116, the version number 118, etc. Other user interface techniques can notify a user of certification. For example, a user interface can play voice data provided by a person who certified the data (e.g., "This web-page was approved by John Doe on February 8, 1999").

FIGS. 1 and 2 illustrate a simple and intuitive interface that ensures presented content is genuine. Underlying mechanisms protect the verification process from being falsified or mimicked. These mechanisms enable users to trust the authenticity of displayed content and provide web administrators with a tool for controlling content offered by a site.

Referring to FIG. 3, a certification process permits an entity (e.g., business, organization, or individual) to establish certification criteria 140. For example, a business can list employees that must approve submitted content 142 before it receives certification. After certification and distribution 144 of content (e.g., by posting the content on an Intranet, Extranet, or Internet site or e-mailing the content to recipients), mechanisms can verify 146 that the content presented to a user satisfies the criteria required for certification 140 and has not been

altered since certification. The process can then present certification information such as the entities that approved the content. Thus, users can view unforgeable information detailing the certification process undergone by content prior to distribution.

Referring to FIG. 4, an illustrative implementation uses a certification server 124 that includes instructions 126 for certifying submitted content 122. The certification instructions 126 can enforce certification criteria (e.g., all content must be approved by the legal department). The certification server 124 can include a database 128 for storing verification information determined from certified content. The verification information includes data that identifies the certified content such as a URL, compressed or uncompressed portions of the content, and/or an assigned identification number. The verification information may also include one or more hash keys (e.g., an MD5 hash and an SHA hash). A hash key is produced by a one-way function and typically requires little storage space (e.g., 160-bits). Hash keys are nearly guaranteed to be unique for any given content.

The database 128 can also store certification information such as the type of certification (e.g., the Legal Department), entities certifying the document, when certification occurred, when certification expires, the version of the certified content, etc. Certification information and verification information are not mutually exclusive categories. A piece of data may be both certification information and verification information.

As shown in FIG. 4, the certification server 124 also includes instructions 132 for processing requests 134 for certification verification. To verify certification, the instructions 132 can compare the verification information 130 stored during certification to verification information determined for the content being verified. A match indicates the content has undergone a certification process and has not been altered since. The certification server 124 can transmit information confirming certification of the content in question, for

example, by dynamically generating HTML instructions that includes certification information. An administrator can revoke certification by simply deleting or altering information in the database 128.

Defining a Certification Procedure

Referring to FIG. 5, an organization can use an interface to define different certifications 148 and criteria for granting the certifications 150 to submitted content. The criteria can include a simple list of employees that must approve submitted content. Criteria can also include programmed logic that tests for satisfaction of different conditions. The ability to program criteria enables a business to define certification processes that reflect a commitment to distributing thoroughly reviewed content.

Referring to FIG. 6, one possible certification scheme 152 uses different certification levels. As shown, the levels include site-wide certification 154, class certification 156-158, and individual certification 160-164. Each defined certification can include its own granting criteria. For example, to obtain site-wide certification, content must first receive certification from the Legal Department 156, the Marketing Department 158, and the company's CEO 164. Similarly, to receive Legal Department certification 156, at least two members of the legal department and a text-scanning program that looks for certain phrases must approve the content. As shown, the certification criteria can include different levels of abstraction. For example, instead of requiring certification from a particular named person, certification criteria can be more abstractly expressed, for example, as a role 162 (e.g., chief attorney) within an organization. This enables certification to continue as different persons fill positions.

The criteria for certification may include different levels of approval. For example, Marketing Department certification 158 may only require that each member of the marketing department receives content for review, while Legal Department certification may require that each member affirmatively indicates

approval of the content. Additionally, certification may be sought for internal (e.g., on an Intranet) or external publication (e.g., on the Internet). The criteria for external publication can be stricter than the criteria for internal publication.

The scheme 152 shown forms a hierarchy between the different certification levels 154-164. The hierarchical structure is a function of the defined criteria and is not an inherent characteristic of schemes having different certifications.

Content Certification

Referring to FIGS. 7A and 7B, easy-to-use graphical user interfaces shield users from the mechanics of submitting content for certification. For example, as shown in FIG. 7A, a user can submit content via a password protected web-page by dragging-and-dropping content onto one or more defined certification controls 156, 158. A control 156, 158 receiving the content can prepare and transmit a certification request indicating the content and the certification desired. The certification controls 156, 158 presented can vary depending on the person submitting content. Alternatively, as shown in FIG. 7B, an application toolbar 171 can include a "Certify" button 173. Selecting the button 173 can prepare and transmit a certification request for a document. The user interfaces of FIG. 7A and 7B are merely illustrative and other differently designed user interfaces could easily provide similar functions. Additionally, a system need not provide a graphical user interface at all, for example, by using e-mail to submit content for certification.

Referring to FIG. 8, a certification request 166 includes content 168 (or a reference to content) submitted for certification and other information 170 such as the certification desired (e.g., site-wide certification or Legal Department certification), the content authors, and a proposed URL. The request 166 can also include information such as a revision number, content keywords, title, etc. (not shown).

SSL (Secure Socket Layer), S-HTTP (Secure Hypertext Transfer Protocol), and other secure communications techniques can protect submitted content from tampering during transmission. Additionally, a request 166 can include one or more digital signatures (not shown) that enable a receiving computer to authenticate the source of the message. While these features enhance security and protect content from tampering en route to the certification server, the certification process does not require these measures.

The certification server 124 can process certification requests. The server 124 can distribute submitted content to individuals 172 that could potentially provide approval needed for certification. For example, the server 124 can distribute content to all the members of the Legal Department when a request is made for Legal Department certification. Workflow software, e-mail daemons, and other techniques, potentially executing on computers other than the certification server, can also distribute content to individuals for certification.

As shown in FIG. 8, after an entity 172 receives and reviews submitted content 168, the entity 172 can notify the certification server 124 of its approval by sending a certification message 174. The certification message 174 can include the submitted content 168 and other information 170 included in the certification request. The message can also include information 174 that describes the person transmitting the certification message 174a, the type of certification granted 174b (e.g., a person can have the capacity to certify content for both the marketing and the legal departments), and a level of approval 174c (e.g., "for internal use only" or "for publication on the Internet"). The certification message 174 may also include a digital signature 176 (e.g., a Verisign™/W3C X.509 digital certificate) belonging to the individual submitting the certification message 174 or may include information used by other authentication techniques such as biometric authentication. As shown in FIG. 8, the certification server 124 processes received certification messages 174 with certifying instructions 126.

Referring to FIG. 9, in one implementation, the certifying instructions 126 authenticate 178 a certification message to ensure the person claiming to have approved submitted content was, in fact, the person who produced the certification message 174. After authentication 178, the instructions 126 can determine 180 whether the certification message received satisfies the criteria for the certification requested. For example, the instructions 126 can determine whether John Doe's 172 certification message 174, alone or in combination with previously received certification messages, is sufficient to obtain Legal Department certification. If the received certification message 174 does not satisfy the criteria, the instructions 126 can store the received certification and await further certification messages. The process may store a hash for submitted content awaiting further certification to ensure that subsequent certification is for the same content as the certification already received. The process 126 can also attempt to certify any links or other objects referenced by the content (e.g., using W3C's manifest protocol).

If the received certification message satisfies certification criteria, the instructions 126 can determine 184 verification information from the certified content or other information provided. For example, the instructions 126 may compute one or more hash keys from the certified content. In general, the verification information can include any information that can be used to identify the certified content.

After storing the content's certification and verification information in the database 186, the instructions 126 can produce a digital signature 188 (e.g., a W3C DSig (Digital Signature Group) compliant signature) for the content 188. The digital signature 208 can include the computed hash 210, the content's URL 212, or any other verification or certification information (not shown).

After producing the digital signature 190, the instructions 126 can determine 190 whether the content can be dynamically modified 192 to include the digital signature. For example, HTML and XML permit dynamic insertion of

digital signatures into content (e.g., as header information or as a newly defined tag). Inclusion of the digital signature in the content ensures that the digital signature travels with the content instead of assuming the signature will remain paired with the content during distribution. The instructions 126 can also dynamically modify the content to include one or more certification indicators 106. The instructions 126 can store the digital signature(s) in its database. This prevents database contents from being tampered with as any altered database information will not match the digital signature(s) stored. Finally, the content and digital signature(s) are distributed by storage at a URL 194, 196 or by sending back the certified content to a submitting user for distribution (not shown).

Referring to FIG. 10, the certification server database 130 includes information corresponding to certified content. This information can include a URL 199, one or more hash keys 200, certifications obtained 201, the certifiers 202, and a certification expiration date 203. The database 130 can also include the location (if any) of previous 204 or later 205 content versions. When the certification server 124 receives a certification verification request, the server 124 can determine whether a user has attempted to access the most recent version of a document. The server 124 can automatically transmit the more recent version of the document to the user. The database can include a wide variety of other information 207 such as a portion of the content and/or a certification expiration date. The database 130 can also include the location of different translations of content and transmit a translation based on "Preferred Language" data included in a certification verification request.

Referring to FIG. 11, after certification, multiple digital signatures 210a, 210b of different certifications may be associated with content. The different digital signatures 210a, 210b may be encrypted and identified by an encapsulating digital signature 208 of the certification server.

Referring to FIG. 12, after content certification, the certification server 124 database 128 stores the verification information 130 corresponding to certified content 168. Referring to FIG. 13, in addition to verifying certification in response to verification requests, the certification process enables an administrator to enforce minimum certification requirements for posted content. For example, a site might define a policy that requires any content available via the World Wide Web to have certification from both the Legal and Marketing Departments. A process 300 can ensure available content meets these requirements 306 by determining the certification possessed by content at each URL 304 offered by a site. Determining content certification can include identifying and verifying digital signatures stored at the URL. Alternatively, the process 300 can determine verification information of a URL and compare the determined verification information with verification information originally stored during certification. Either technique ensures that employees or others do not post content without receiving sufficient certification.

Referring to FIG. 14, enforcing certification criteria can instead occur at a web-server processing content requests. After receiving a request for content 303, the web-server can determine 305 if the requested content has the certification required for transmission 309. If not, the web-server can notify the web-server administrator 307 that insufficiently certified content has been requested indicating that a link or directory has indicated the presence of the content on the server. This enables the administrator to quickly find content that should not be posted at the site. The web-server can also store information that specifically disavows certification for particular content.

Certification Verification

Referring to FIG. 15, in one implementation, certification instructions dynamically modify certified content to include one or more certification indicators 106a, 106b. Referring to FIG. 16, certification indicators 106c, 106d

may instead be paired with a listing of certified URLs 107c, 107d, for example, produced by a search engine. The certification indicators 106a, 106b may be packaged (e.g., included in the same ActiveX control or Java applet) with a corresponding URL 107a, 107b to prevent a certification indicator 107a, 107b from accidental or intentional pairing with a different, potentially uncertified, URL. Selecting an indicator 106, 106a, 106b can initiate a certification verification process.

Referring to FIG. 17, initiation of the certification verification process can include preparing and transmitting a certification verification request 221 to a certification server. The request 221 can include, for example, the certification claimed by a certification indicator 223 and verification information 225 determined from the content presented. The request may be encrypted to prevent analysis. The request 221 may also include a portion of the content presented 227 for comparison to similar information stored in the certification server. This can make "door-knob rattling" more difficult. That is, people wishing to find a valid hash key cannot simply submit request after request with different hash keys until one works. The request 221 can include other information such as the URL of the content, etc.

Referring to FIGS. 18-22, certification verification can be implemented in any number of ways. The techniques used to verify certification can depend in part on functions provided by the browser (or other application) presenting the content in question. For example, older browsers may not accept or be able to process digital signatures. Additionally, a browser may not include instructions for determining verification information (e.g., the ability to compute an MD5 hash from presented content).

The different certification verification techniques, nevertheless, share a general process 132. First, the procedures 132 determine verification information (e.g., computing a hash or extracting verification information from a digital signature) for content 220 being verified. When the determined

verification information matches 222, 224 the verification information originally determined during certification, the procedures 132 can conclude that the content satisfies certification criteria and has not been altered since certification. The procedures 132 may also check to ensure certification has not expired and that a more recent version of the document has not been certified.

After verifying certification, the procedures 132 can cause display of verification and/or certification information such as the entities that certified a document, when certification occurred, etc. Similarly, the procedure 132 can notify a user if verification fails. The procedures 132 can also cause other programmatic behavior to occur in addition to or in lieu of causing a display of information. A small subset of possible implementations follows.

Referring to FIG. 19, if a browser has access to digital signature(s) produced during certification and the ability to determine verification information from content, the browser can extract the verification information from the digital signature(s) 230, determine the verification information of the content in question 232, and compare the two 234. A match verifies the claimed certification 236. This method does not require access to the certification server for certification verification. However, access to the certification server enables a user to determine if the content remains certified or has been replaced by a new version.

Referring to FIG. 20, if a browser does not have access to digital signature(s) produced during certification but has the ability to determine verification information, the browser can determine the verification information for the content 240 (e.g, compute a hash) and send the determined verification information to the certification server 242. The certification server can compare 244, 246 the determined verification information with the verification information originally determined during certification. Again, if the two match, the content's certification has been verified.

Referring to FIG. 21, in some cases, content may not display a certification indicator. A user may, nevertheless, determine whether the content

received certification. In one implementation, the user can visit a certification server web-site 252 and enter a URL for verification 254. Instructions on the certification server can collect the content provided by the resource at the identified URL, determine verification information from the collected content 256, and compare the determined verification information with stored verification information of certified content. If the instructions find a match, the instructions can transmit verification and/or certification information to the user.

Referring to FIG. 22, in another implementation, a user can simply transmit content in question to the certification server 266 for certification verification. The certification server determines verification information for the content 268 and can compare 270 this verification information with verification information stored in its database. If the certification server identifies a match 272, the certification server can transmit the verification and/or certification information to a user for display 274.

Each of the implementations described above enables a user to quickly determine whether presented content actually comes from an official source. This enables a user to place greater reliance on the presented information and can make the user more likely to return to a site. The implementations also enable a content provider to closely scrutinize and guard the content it distributes.

Multiple Certification Servers

Referring to FIG. 23, the previous discussion described a single certification server. The techniques described can also be used with a network of certification servers. Certification server instructions 322 can be transmitted to different computers requesting 320 the instructions. Such transmission can occur after financial arrangements have been settled. Additionally, authentication may be performed by both the requesting and transmitting servers.

Referring to FIG. 24, certification servers may form a hierarchy 324. For example, a root certification server 326 connects to different company

"Headquarter" certification servers. For example, server 328 may belong to Honda while server 330 belongs to General Motors. Each of the headquarter servers may connect to different divisions within a company. For example, server 332 may belong to Honda Motorcycles while server 334 belongs to Honda Automobiles. Although FIG. 24 illustrates a hierarchical relationship, other certification server topologies are possible.

Hierarchically organized certification servers permit distribution of server processing and storage over a number of computers without losing the ability to verify content certified by any of the servers. Additionally, the structure permits hierarchically higher servers to control functions performed by lower servers. For example, a server can control whether another server is itself able to make a request for certification software.

For example, referring to FIG. 25, a recursive procedure 336 can quickly search each certification server to verify certification of content in question. After receiving a verification request 338, a certification server can check its own database 340 for verification information corresponding to the verification request 338. If unable to find the verification information in its own database, the server can issue a verification request to connected servers 344. Eventually, a verification request will reach the server used for certification of the content 342 or all servers will return an indication that no server has certified the content in question.

Other procedures can go up the hierarchy rather than down. For example, when a division certification server 332 receives a certification verification request it cannot provide, the division server 332 can issue a certification verification request to the headquarter's certification server 328.

Franchising

A franchisor (e.g., a corporation or syndicated) often may want to provide content for display on its franchisee's Web-sites. For example, General

Motors may want local dealerships to include a national sales advertisement. Additionally, franchisees may want to download certified content describing new products.

Referring to FIG. 26, a franchisor 350 (e.g., a corporation or syndicate) can provide content to different franchisees 352, 354. Any given site may act as both a franchisee and franchisor (not shown).

Referring to FIG. 27, after establishing a franchisor/franchisee relationship, a proxy is established at the franchisee with which the franchisor can communicate to manage content including refreshing and invalidating content. Thereafter, a franchisee can request content from the franchisor 356. After authenticating the franchisee's request 357, the franchisor can send the requested content, digital signatures associated with the content, and verification information determined for the content during certification 358. The franchisee can store the downloaded information and provide the content to site visitors 360.

Referring to FIG. 28, a franchisor can control the content offered by its franchisees. For example, to de-certify or update content, the franchisor can download replacement content or the franchisor can mark the content in the proxy invalid. When a franchisee receives a request for invalid content 364, the franchisee requests updated content from the franchisor 366. The franchisor can monitor the content offered by its franchisees by examining verification information corresponding to the content or the content itself.

After downloading information from a franchisor to a franchisee Web-server, visitors to the franchisee can view the downloaded content. The franchisee proxy can automatically transmit a certification verification request each time a visitor requests content.

Requests for content can be metered by the franchisee proxy. Thus, a franchisor can receive reports regarding which franchisee sites reached the most customers. Metering data can be used for analytical purposes or even as a way to charge for use of content (e.g., for each web-page hit) or pay for its distribution.

For example, metering can be used as a way for franchisees to charge franchisors for distribution of content, for example, by charging a small fee for each content request.

Alerting Users of Content Validation

FIG. 29 again shows a web-page 1100 presented by an Internet browser. A user viewing the page 1100 often must trust that the content-provider stands behind the contents and/or that the contents have not been tampered with. Sometimes this trust is misplaced. For example, someone may have posted the content at the business' web-site without appropriate approval (e.g., undergoing a certification process). Alternatively, some intermediate network node may have intercepted content as it traveled across the Internet and replaced selected portions.

This application describes techniques that enable a content provider to certify content. This application also describes techniques for validating certification of downloaded content. Such validation can include determining content is not certified, determining content was altered after certification, determining certification has expired, and/or determining certification has been revoked. Such validation can also include determining and authenticating the identities of entities claiming to have certified the content. As shown in FIGS. 30-36, these techniques have been embodied in a software program that can use graphical indicators, sound, and other notification techniques to notify a user whether downloaded content is certified content.

Display of Certification Status

A number of different mechanisms can notify users of whether downloaded content is certified content. For example, FIGS. 30 and 31 show a Microsoft® Windows 95 taskbar button 1104 and tray icon 1106 that change appearances based an attempt to validate certification of content displayed in an

active browser window. For example, the controls 1104, 1106 may notify a user of the certification status (e.g., certified, uncertified, expired, revoked, etc.) of content using text, graphics, color, and other display attributes. The appearance of the controls 1104, 1106 may vary in different ways for different certification statuses. For example, content that was never certified may cause the tray icon to display a bright red skull and cross bones to alert a user, while content having revoked certification may cause the tray icon to turn orange. The unobtrusive placement of the controls 1104, 1106 provides real-time, continual, notification of content certification without interfering with a user's normal browser interaction.

FIGS. 32-35 show a number of other user notification techniques. For example, FIG. 28 shows a window 1108 that displays a map 1110 of content displayed by a browser. The map 1110 may include a logo (not shown) of the site offering the content. The different appearances of map regions indicate the certification status of content. For example, red portions may indicate uncertified regions of a page, while white portions may indicate certified regions. The window enables a user to quickly identify potentially uncertified content.

FIG. 33 shows a window 1112 that displays a tree of web-page contents 1114-1120. Each node in the tree can correspond to a different content (e.g., a node for a page's HTML and nodes for different GIF (Graphics Interchange Format) pictures referred to by the page). Again, different display attributes of tree nodes reflect the certification status of content. For example, shaded node 1116 indicates that the picture for "Digests of Patent Opinions Federal Circuit" has not been certified. The map of FIG. 32 and the tree of FIG. 33 can provide a user with a visual description of content certification, without altering the browser's display of the page or otherwise altering the browser's functions.

Other techniques, however, use browser-provided functions to provide an indication of the certification status of content. For example, as shown in FIG.

34, a browser may be dynamically programmed to display the certification status of content on a page as a user brushes the content with a cursor. For browsers not offering this capability, this feature may be offered by continuously determining cursor placement and displaying a window near the content. Alternatively, the window may only be displayed when a user selects content, for example, by clicking a mouse button on the content.

As shown in FIG. 35, software can also directly alter the display of contents after determining the certification of different portions. For example, as shown, the software can black-out 1114 uncertified content, and/or alter the display of content 1116 having expired certification. Depending on the browser, this may require writing a downloaded page to a temporary file, modifying the temporary file, and reloading the modified temporary file into the browser.

The embodiments described above can also provide more detailed information about the certification of content. For example, by selecting the system taskbar button 1104 in FIGS. 30 or 31, a dialog, as shown in FIG. 36, can display detailed information about content. The detailed information can include the certifying entity 1124, a graphic for the entity (e.g., a business trademark), the trustworthiness of the page or content 1125, the URL (Universal Resource Locator) or URI (Universal Resource Indicator) of the content 1127, the range of dates the certification is valid 1128, and a "digital fingerprint" of the content 1129. The dialog may also display other information (not shown) such as the site certificate of the web-site providing the page and potentially a text description of the "Trust Policy" used by the site to certify content (e.g., "Factpoint, Inc. uses a five person review board to certify content prior to posting").

Any of the visual techniques described above can be combined and/or used in conjunction with non-visual techniques such as audio messages (e.g., "The picture of Abe Lincoln is untrustworthy"). Additionally, while the above description described individual pages, the same techniques work equally well with framed browser displays that display two or more pages simultaneously.

Underlying the displays shown in FIGS. 30-36 are certification procedures that enable providers to certify posted content and validation procedures that enable users to validate the certification of received content.

The Trust Validator

FIG. 37 shows a client 1136 browser 1140 downloading information (i.e., page 1132) from a URL (Universal Resource Locator) 1132 over a network 1144. The client 1136 can present the downloaded content on a user's monitor 1142, speaker, etc. As shown, the client 1136 includes "trust validator" software 1138 that validates certification of downloaded content. The validator 1138 may operate as a background process that monitors content received by the browser 1140, for example, via calls to or from the browser API (application programming interface). Alternatively, validator 1138 functions may be directly integrated into the browser 1140.

The validator 1138 can validate content certification using certification information associated with the content. For example, the validator 1138 can compare certification information determined for the content determined prior to transmission to the client with certification information determined after transmission.

In more detail, a certification process produces certification information 1134 based on the certified content(s). Typically, this information 1134 is produced using a "one-way" function. For example, a hashing function may use all or some portion of the ASCII characters in HTML (HyperText Markup Language) commands that define a page to produce a set of output bytes. Given the same input, the hashing function produces the same output. A popular hashing functions known as MD5 and SHA can produce relatively small output for large pages.

The certification information 1134 derived from the content may be included in the content itself, for example, as data, for example, as signature

and/or manifest elements of an XML (Extensible Markup Language) page or as an HTML "Meta" element. When the certification information 1134 is included in the content, it must be removed before re-determining the certification information.

Alternatively, the information 1134 may be included in the header of an HTTP (HyperText Transfer Protocol) message sent by the server 1130. In yet another implementation, the trust validator 1138 may independently request certification information 1134 for the downloaded content. For example, the site may provide a file (e.g., "factpoint.txt") at a predefined location (e.g., "www.url.com/factpoint.txt") that lists where certification information 1134 for site content can be found. The file may refer to other sites when the content has been copied.

FIG. 38 shows a process 1138 the trust validator can use to validate certification of downloaded content. First, the trust validator obtains 1150 the downloaded content (e.g., a page or portion of a page) and the certification information associated with the content. The trust validator 1138 can obtain this information from the browser 1140 or can establish an independent connection with the server 1130. The trust validator 1138 can independently determine certification information using 1152 the one-way function on the received content. By comparing 154 the received certification information and the independently determined certification information, the validator 1138 can determine 1154 whether the page 1132 has been altered since certification and notify a user of such a change. The trust validator may also notify a web-site administrator if certification validation fails so the administrator can investigate uncertified content offered by the site.

FIG. 39 shows a scheme that can not only detect tampering, but that can also identify and authenticate the entity or entities certifying content. This scheme features certification information that includes a hash digitally signed by one or more certifying entities. A digital signature 1160, much like a handwritten

signature on a piece of paper, provides a degree of certainty that a particular entity signed the content in question.

One digital signature scheme uses a private encryption key known only to the signer and a public encryption key that may be freely distributed. Information encrypted with the private key can only be unencrypted with the public key. Thus, an entity certifying content can encrypt a hash of the content with their private key. Only the public key associated with the entity can properly decrypt the hash. For example, a hash of content may be encrypted using a private key assigned to a web-site and decrypted using a public key included in the site's certificate. A wide variety of other digital signature schemes may be used such as an exchange of a single encryption key or the use of physical devices such as smart cards.

In the system of FIG. 39, information needed to validate a digital signature may be included with the certification information. The information may include an X.509 certificate for each entity signing the hash. For example, an X.509 certificate may include the public key needed to decrypt the hash of the page 1132, a description of the entity holding the private key, and the digital signature of some authority such as VeriSign® testifying to the truth of the information in the certificate (i.e., that the entity claiming to have signed the hash is actually the claimed entity). In another embodiment, the information needed to validate a digital signature (or a reference to this information) may be provided by one or more DSig (Digital Signature Users Group) digital signature blocks.

As shown in FIG. 40, after receiving the certification information (e.g., digital signature and certificates), the trust validator 1138 can use the public key included in the certificate to extract the hash included in the digital signature. The trust validator 1138 can also follow the chain of authority 1162, for example, by asking VeriSign® if the public key received is really the public key of the entity claiming to have signed the hash. The trust validator can include information about the chain of authority in a display such as the dialog shown in

FIG. 36. After extracting the hash from the certification information, the trust validator 1138 can conclude the page was altered or was never certified to begin with and can notify a user using the techniques described above.

If the certification information includes a digitally signed hash, the certification information may be transmitted over an insecure connection. If, however, the certification information only includes a hash, a secure connection such a secure sockets layer (SSL) connection may be preferred.

As shown in FIG. 41, instead of a single digital signature or hash, certification information may include a manifest 1170 for content included in a page. The manifest 1170 itself may be hashed and digitally signed. As shown in FIG. 42, the manifest 1170 can include the hash values of different page 1130 content. For example, the manifest 1170 shown includes a different hash value for each picture displayed on the page. The trust validator 1138 can use this information to validate each portion of a page individually. The validator 1138 can also use criteria to produce an overall estimation of page certification. This criteria may be provided by rules included in the manifest 1170 (e.g., defining valid content collections), logic hard-coded into the validator, and/or as logic provided by user-supplied code (e.g., a Java script). By default, the validator 1138 can describe the page as having the lowest certification status of any content in the page. For example, if any content on the page has expired, the page as a whole is deemed expired. The validator 1138 may use similar logic for frames. That is, the overall certification status of a display is determined by the worst certification status of any content in any displayed frame.

In some implementations, the trust validator 1138 can alert a user to revocation, expiration, and other certification statuses of downloaded content. FIG. 43 shows a server 1130 that includes a database table 1182 describing available content 1132. The table 1182 can include an expiration date for certification, a blanket revocation of certification, and other information. Upon receiving content, the trust validator 1138 can transmit a validation request to

validation software 1180 on the server 1130. The validation software 1132 can access the table 1182 to verify the content was certified and determine whether the content has expired or has been revoked. The validation software 1132 can transmit the results back to the trust validator 1138.

Though information in the table 1182 may be included in the certification information received by the client, the table 1182 enables an administrator to centrally alter certification information. The server table 1182 can also be used to provide content "versioning". For example, a web-site may certify a more recent version of information for a URL. Validation software can look for valid versions of a URL when a client attempts to validate expired or revoked content.

FIG. 44 describes this validation process in greater detail. After receiving the content and its corresponding certification information 1200 and independently determining the certification 1204 for the content, the validator 1138 can preliminarily determine if the content is certified without accessing the server 1130. For additional validation, the validator 1138 can also transmit 1206 certification information (e.g., the hash) to the server validation software for look-up in the server table 1182. The server table 1182 can not only verify that the content has not expired or been revoked, the server table 1182 can also identify more recent content that replaces the content the user downloaded (e.g., the URL for the hash submitted has another table entry that has not been revoked). The trust validator can then establish a connection to download the valid version for display in the browser.

FIG. 45 shows a secure architecture that distributes server certification and validation functions between a certification server 1218 and a validation server 1232. The certification server 1218 includes certification software 1220 that certifies submitted content 1214. The certification server 1218 also adds table 1182 entries as content is certified.

An administration tool 1216 can manage information stored in the table, for example, to specify an expiration date, delete certification, or revoke certification for content.

The certification software 1220 may certify a single piece of content or a collection of web-pages using a certification "spider." Certification may be performed for fixed or dynamically constructed content. After certification, the certification server can place certified content on the validation server for distribution.

The validation server 1232 includes validation software 1228 that accesses the certification server 1220 table 1182 in response to client validation requests. The validation server 1232 may maintain a cache of validation data to reduce the time spent serving client requests.

Embodiments

The techniques described here are not limited to any particular hardware or software configuration; they may find applicability in any computing or processing environment. For example, functions described as being performed by a certification server can be distributed across different platforms.

The techniques may be implemented in hardware or software, or a combination of the two. Preferably, the techniques are implemented in computer programs executing on programmable computers that each include a processor, a storage medium readable by the processor (including volatile and non-volatile memory and/or storage elements), at least one input device, and one or more output devices. Program code is applied to data entered using the input device to perform the functions described and to generate output information. The output information is applied to one or more output devices.

Each program is preferably implemented in a high level procedural or object oriented programming language to communicate with a computer system.

however, the programs can be implemented in assembly or machine language, if desired. In any case, the language may be a compiled or interpreted language.

Each such computer program is preferably stored on a storage medium or device (e.g., CD-ROM, hard disk or magnetic diskette) that is readable by a general or special purpose programmable computer for configuring and operating the computer when the storage medium or device is read by the computer to perform the procedures described in this document. The system may also be considered to be implemented as a computer-readable storage medium, configured with a computer program, where the storage medium so configured causes a computer to operate in a specific and predefined manner.

Other embodiments are within the scope of the following claims.

What is claimed is:

1. A method of processing content, comprising:

storing verification information corresponding to certified content at a first computer;

receiving a verification request corresponding to content from a second computer;

determining verification information for the content corresponding to the verification request; and

comparing the determined verification information with the stored verification information.

2. The method of claim 1, further comprising, receiving content certification criteria.

3. The method of claim 2, wherein certified content comprises content satisfying the content certification criteria.

4. The method of claim 2, wherein content certification criteria comprises a list of required approval.

5. The method of claim 2, wherein content certification criteria comprises programmed logic.

6. The method of claim 1, further comprising storing certification information.

7. The method of claim 6, wherein certification information comprises at least one of the following: a type of certification granted, entities approving certification, and when the content was certified.

8. The method of claim 1, wherein verification information comprises information derived from the content.

9. The method of claim 8, wherein information derived from the content comprises at least one hash key.

10. The method of claim 1, wherein the verification request includes a URL (Uniform Resource Locator).

11. The method of claim 10, wherein determining verification information comprises collecting content from the URL included in the verification request.

12. The method of claim 1, wherein the verification request includes content.

13. The method of claim 12, wherein determining verification information comprises determining verification information for the content included in the verification request.

14. The method of claim 1, wherein the verification request includes verification information.

15. The method of claim 14, wherein determining verification information comprises using the verification information included in the verification request.

16. The method of claim 1, wherein receiving a verification request comprises receiving a request caused by user interaction with a certification indicator.

17. The method of claim 16, wherein the certification indicator is included in the content.

18. The method of claim 16, wherein the certification indicator comprises a graphic image having associated instructions that produce a verification request.

19. The method of claim 1, further comprising transmitting certification information to the second computer.

20. The method of claim 1, wherein the content comprises at least one of the following: graphics, text, animation, sound, and instructions.

21. The method of claim 1, wherein the content comprises a web-page.

22. The method of claim 1, wherein comparing comprises issuing verification requests to connected certification servers.

23. A method, comprising:

presenting an indication that content has received certification;

receiving user input requesting verification that the content has received the certification indicated;

transmitting a certification verification request to a certification server; and

receiving information describing whether the content has actually received the certification presented by the indication.

24. The method of claim 23, wherein presenting an indication comprises presenting a user interface control.

25. The method of claim 24, wherein receiving user input comprises receiving user input via the user interface control.

26. The method of claim 23, further comprising displaying information included in the information received.

27. The method of claim 23, wherein the information received comprises at least one of the following: content authorship, revision number, expiration date, and type of certification.

28. The method of claim 23, wherein transmitting a certification verification request comprises transmitting verification information determined from the content.

29. The method of claim 28, wherein the verification information comprises a hash key.

30. The method of claim 23, wherein transmitting a certification verification request comprises transmitting information included in the content.

31. The method of claim 23, wherein transmitting a certification verification request comprises transmitting a URL.

32. A method of controlling content distribution, comprising:

receiving certification requirements for content to be distributed;

identifying content to be distributed; and

determining whether the identified content satisfies the received certification requirements.

33. The method of claim 32, wherein identifying content comprises receiving a request for content.

34. The method of claim 32, wherein identifying content comprises collecting content from a set of locations.

35. The method of claim 32, wherein the determining comprises identifying at least one digital signature associated with the content.

36. The method of claim 32, wherein the determining comprises determining verification information for the content.

37. A method of processing content received from a networked computer in response to a browser request for content, the method comprising:

receiving certification information associated with content received by the browser;

determining a certification status for content based on the received certification information; and

displaying at least one indication of the determined certification status of the content.

38. The method of claim 37, wherein the indication comprises a persistant indication displayed with the content.

39. The method of claim 37, wherein the indication comprises a taskbar button.

40. The method of claim 37, wherein the indication comprises a tray icon.

41. The method of claim 37, wherein displaying at least one indication comprises processing the content to include one or more indications.

42. The method of claim 41, wherein processing the content comprises altering visual representation of the content.

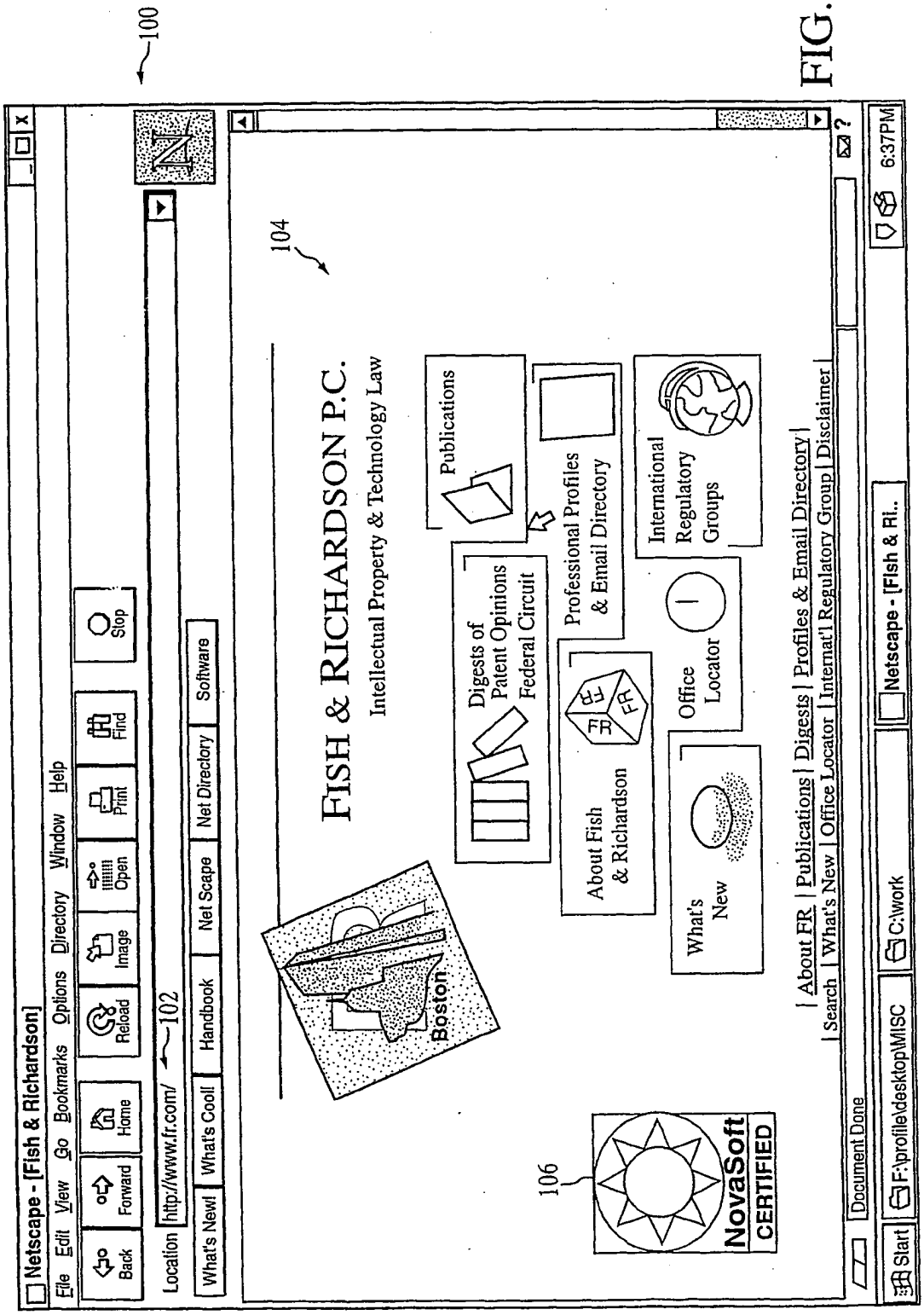


FIG. 1

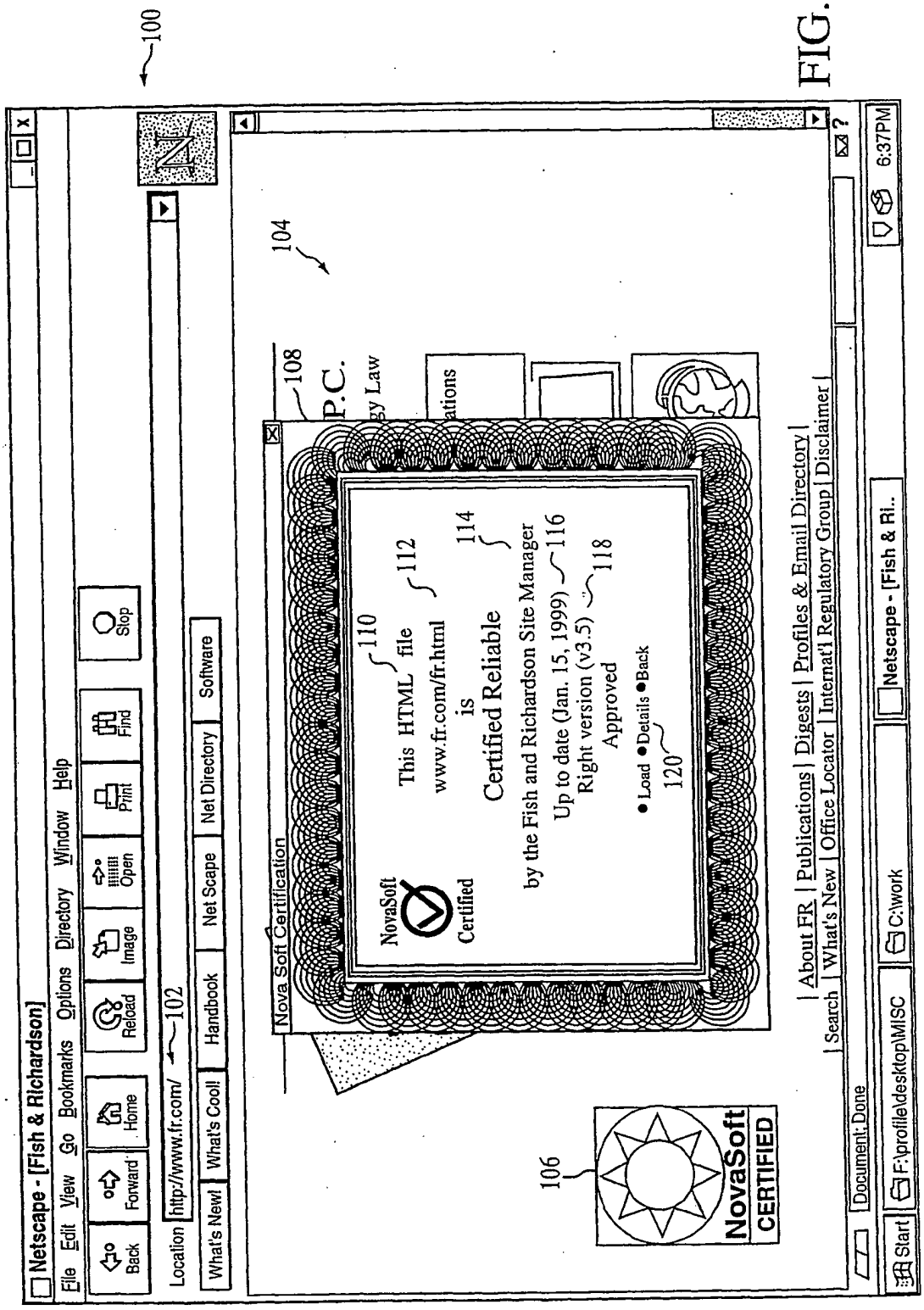


FIG. 2

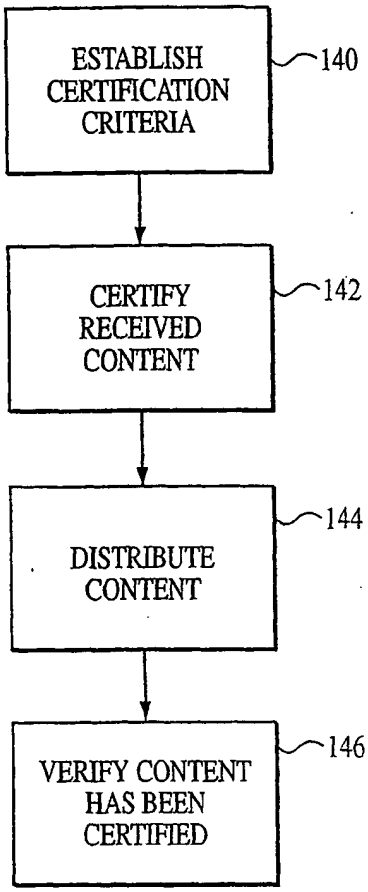


FIG. 3

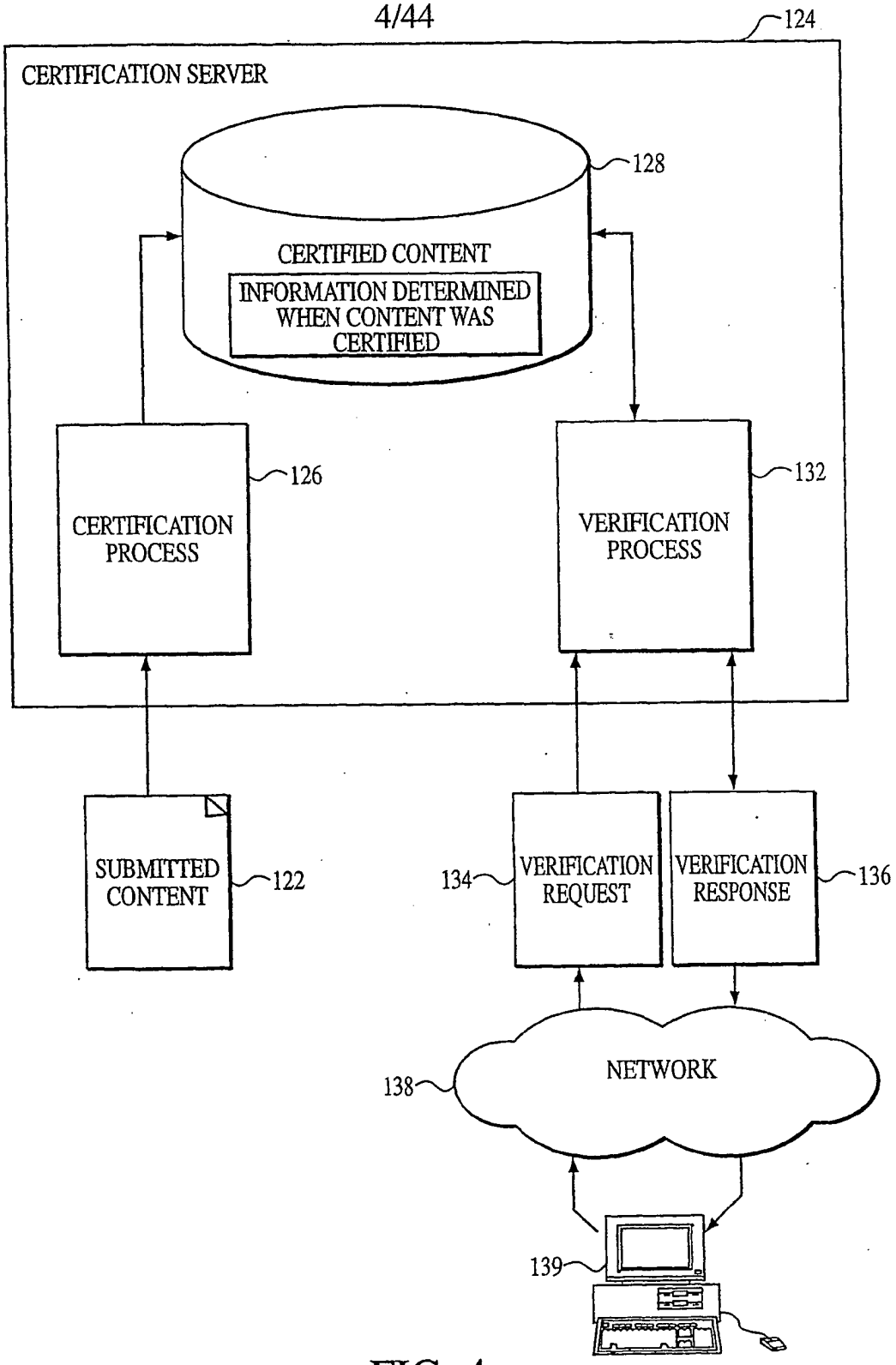


FIG. 4

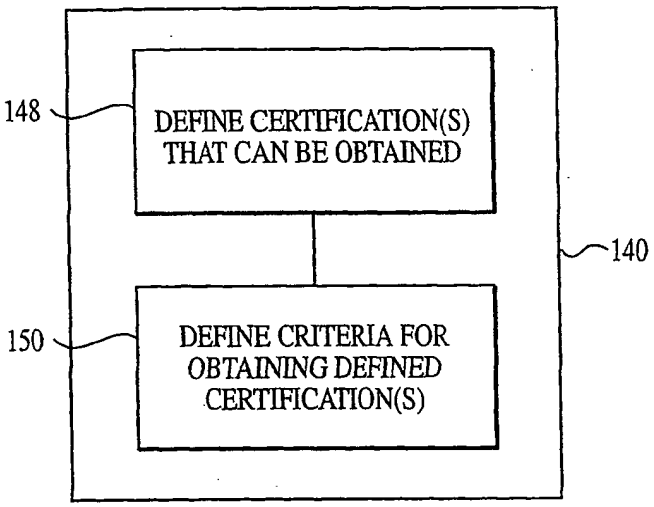


FIG. 5

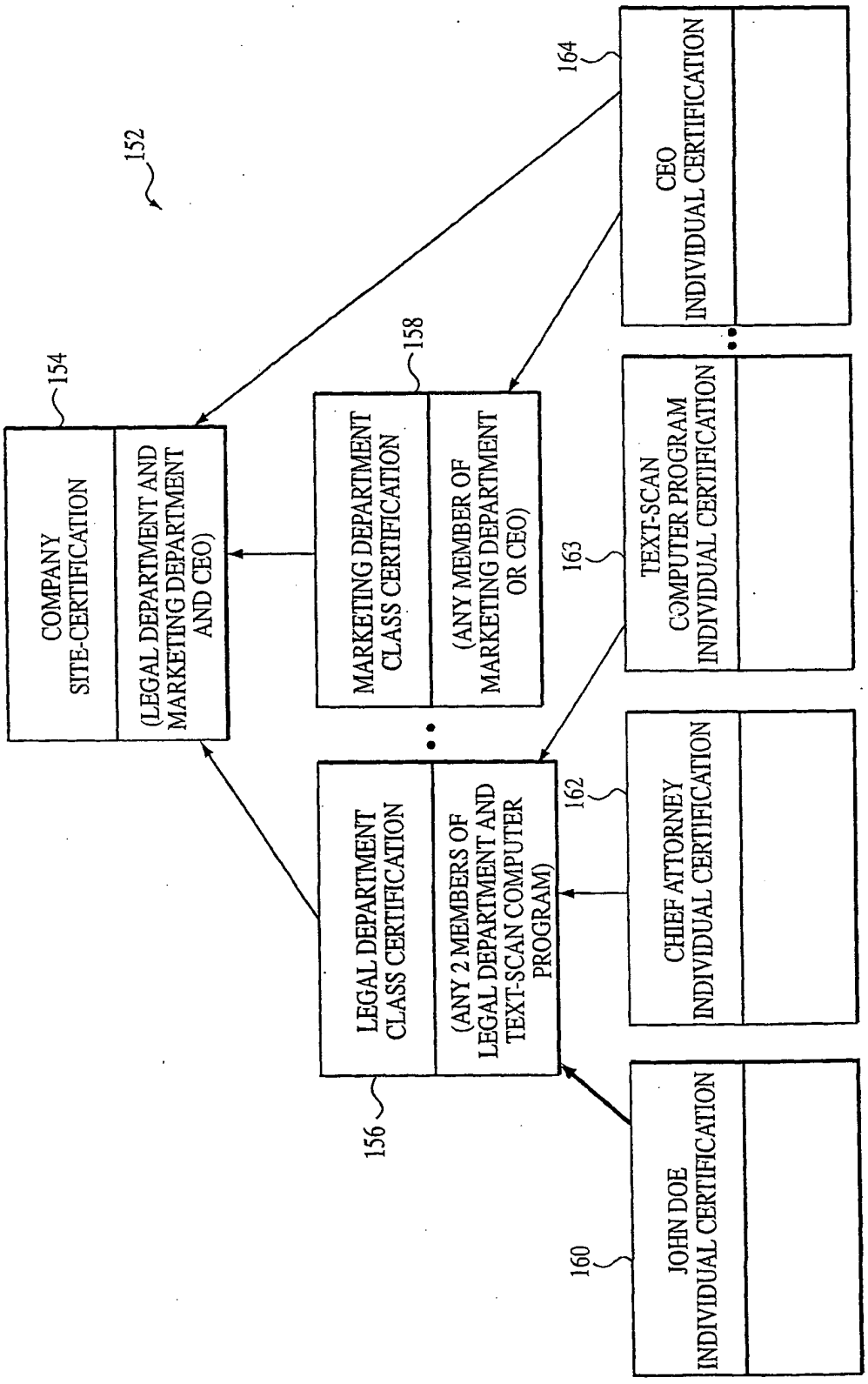


FIG. 6

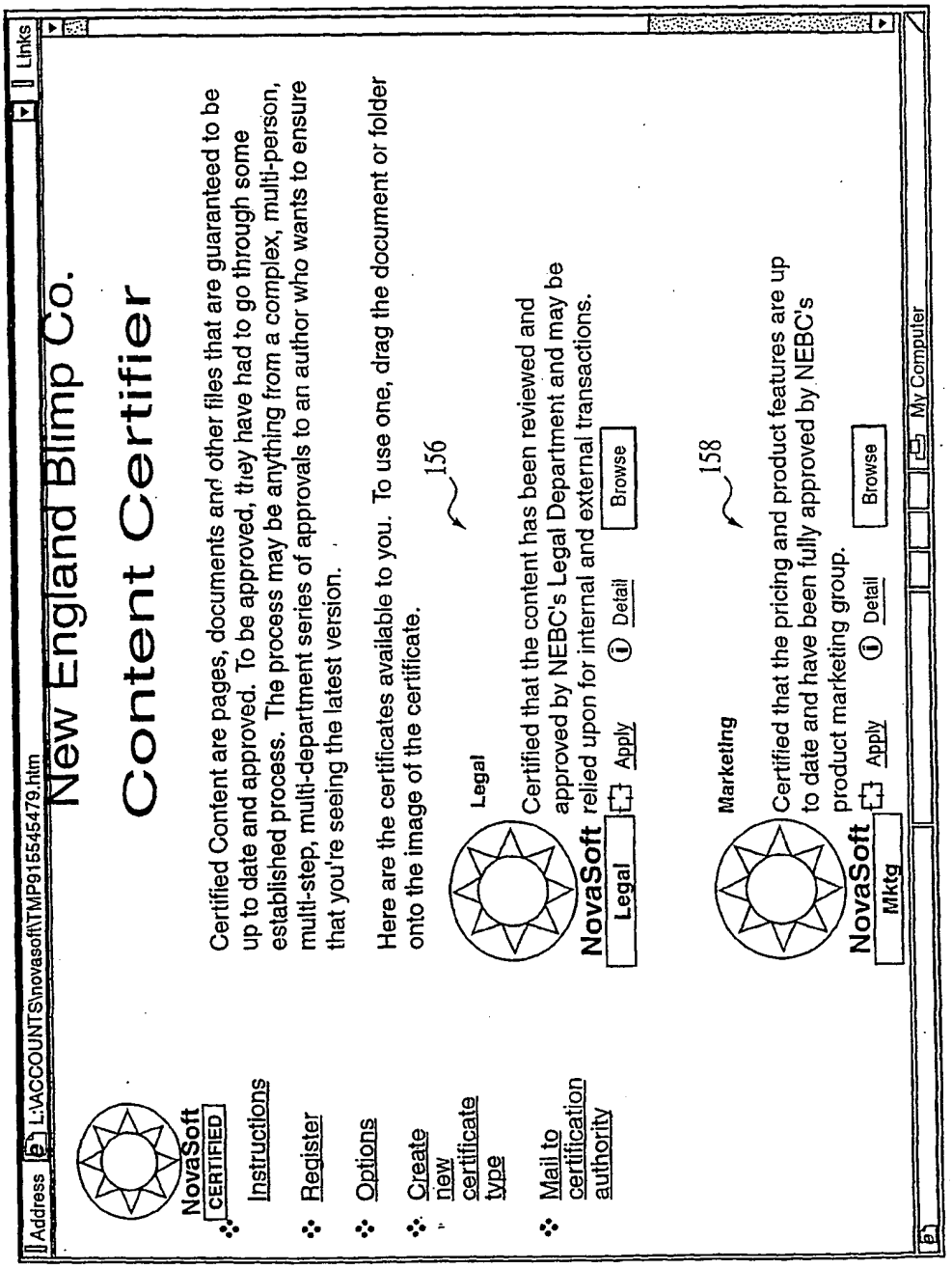


FIG. 7A

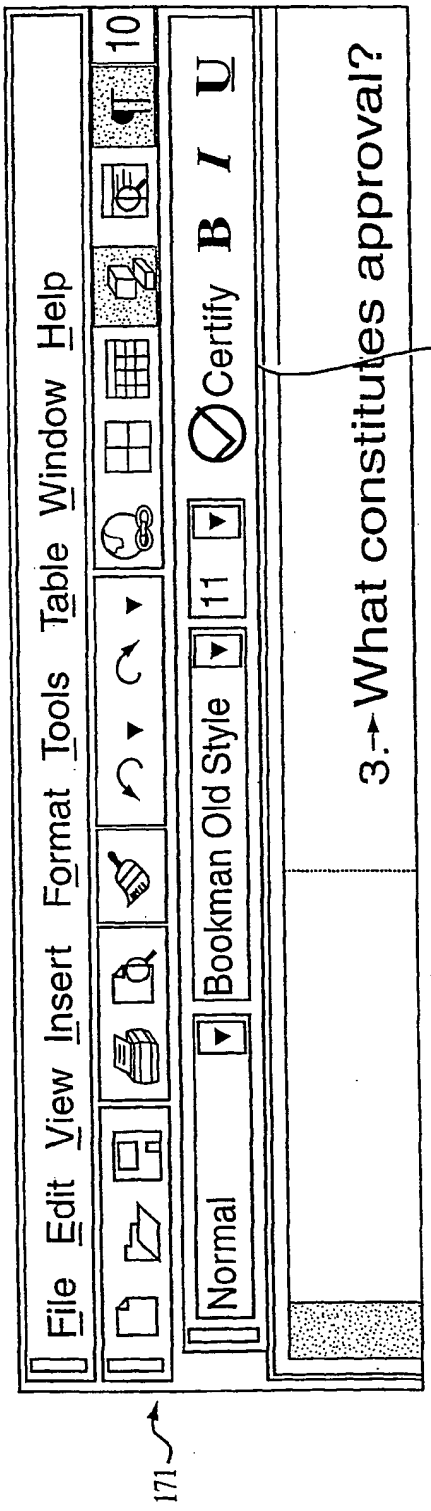


FIG. 7B

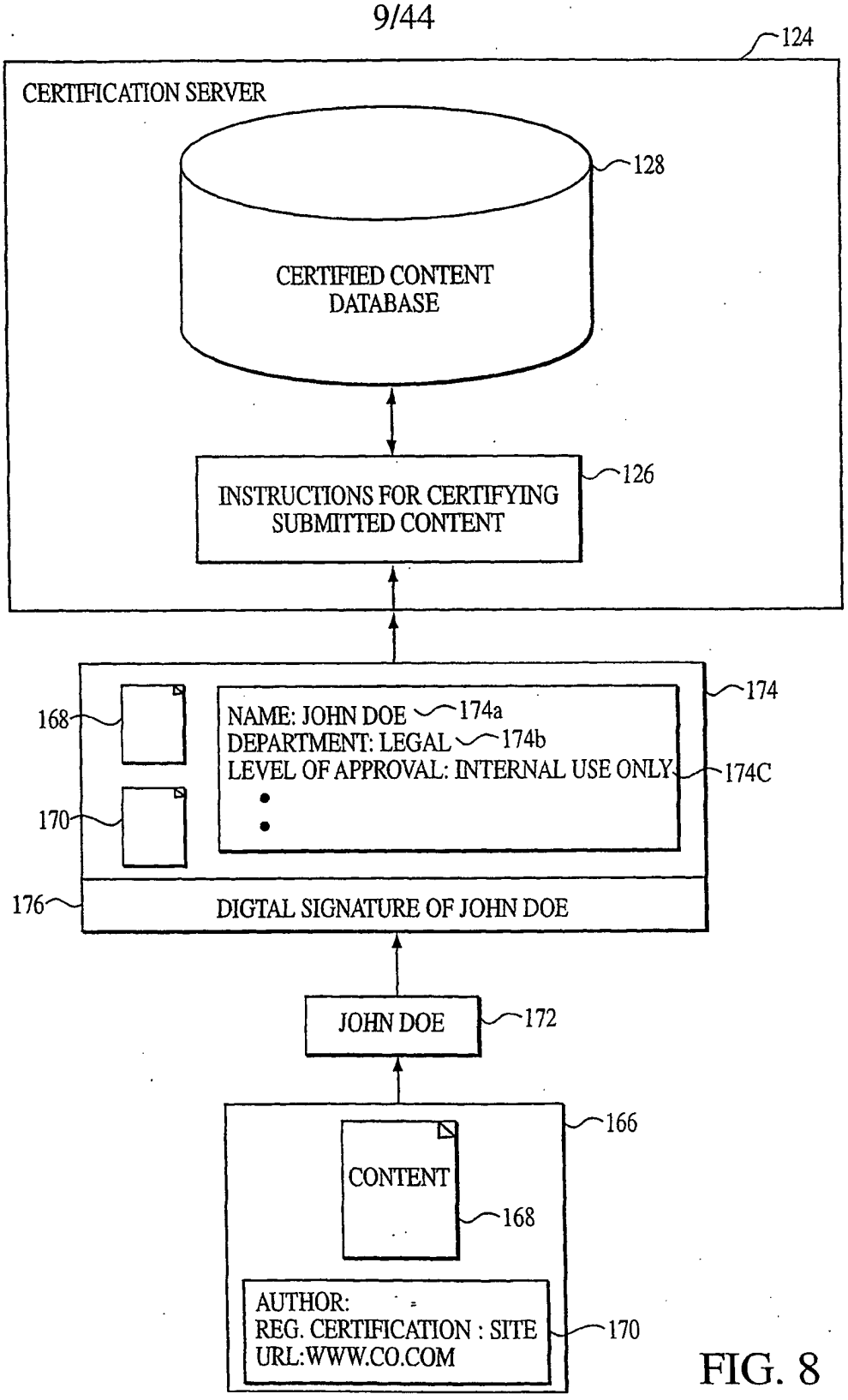


FIG. 8

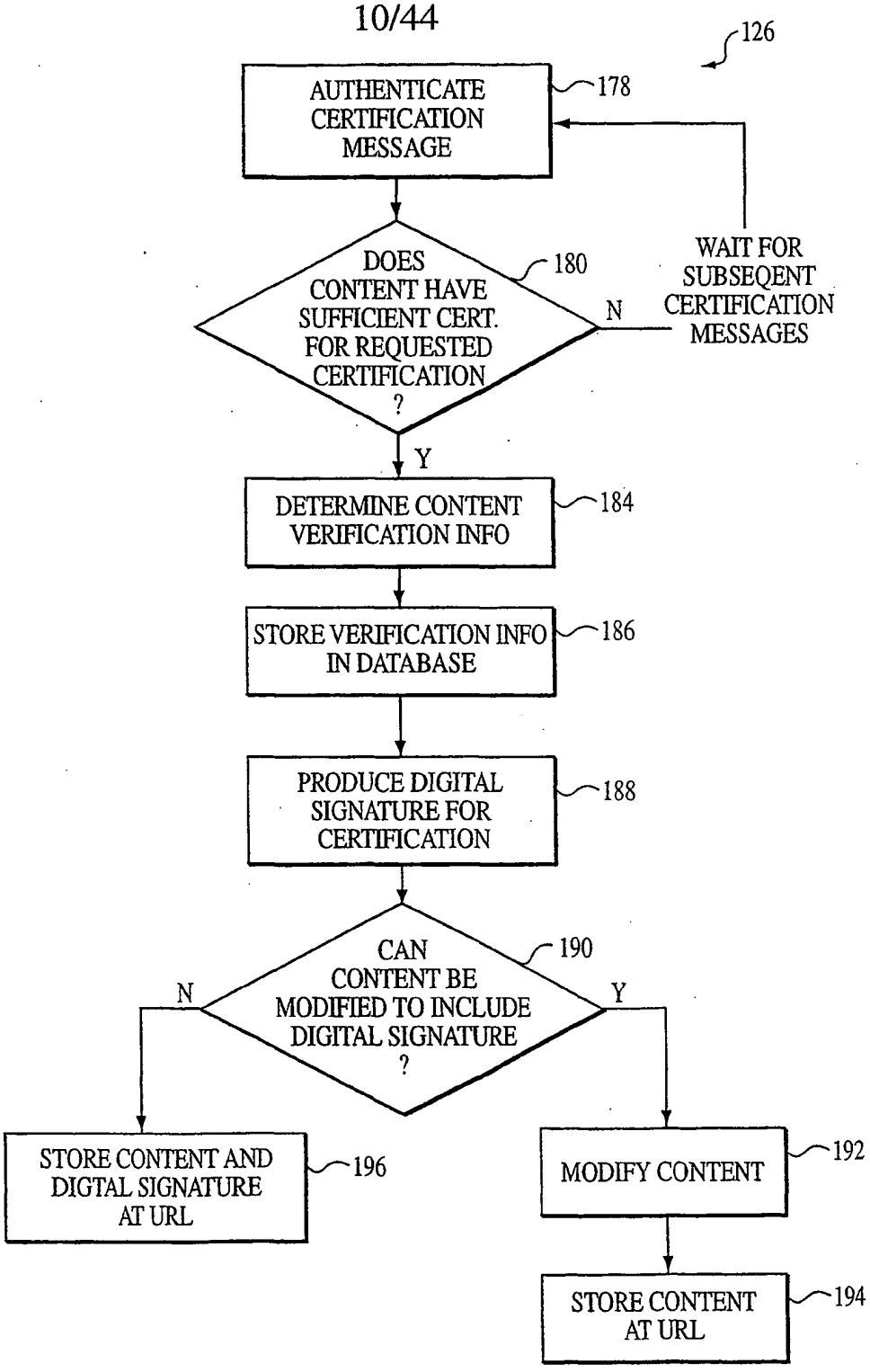


FIG. 9

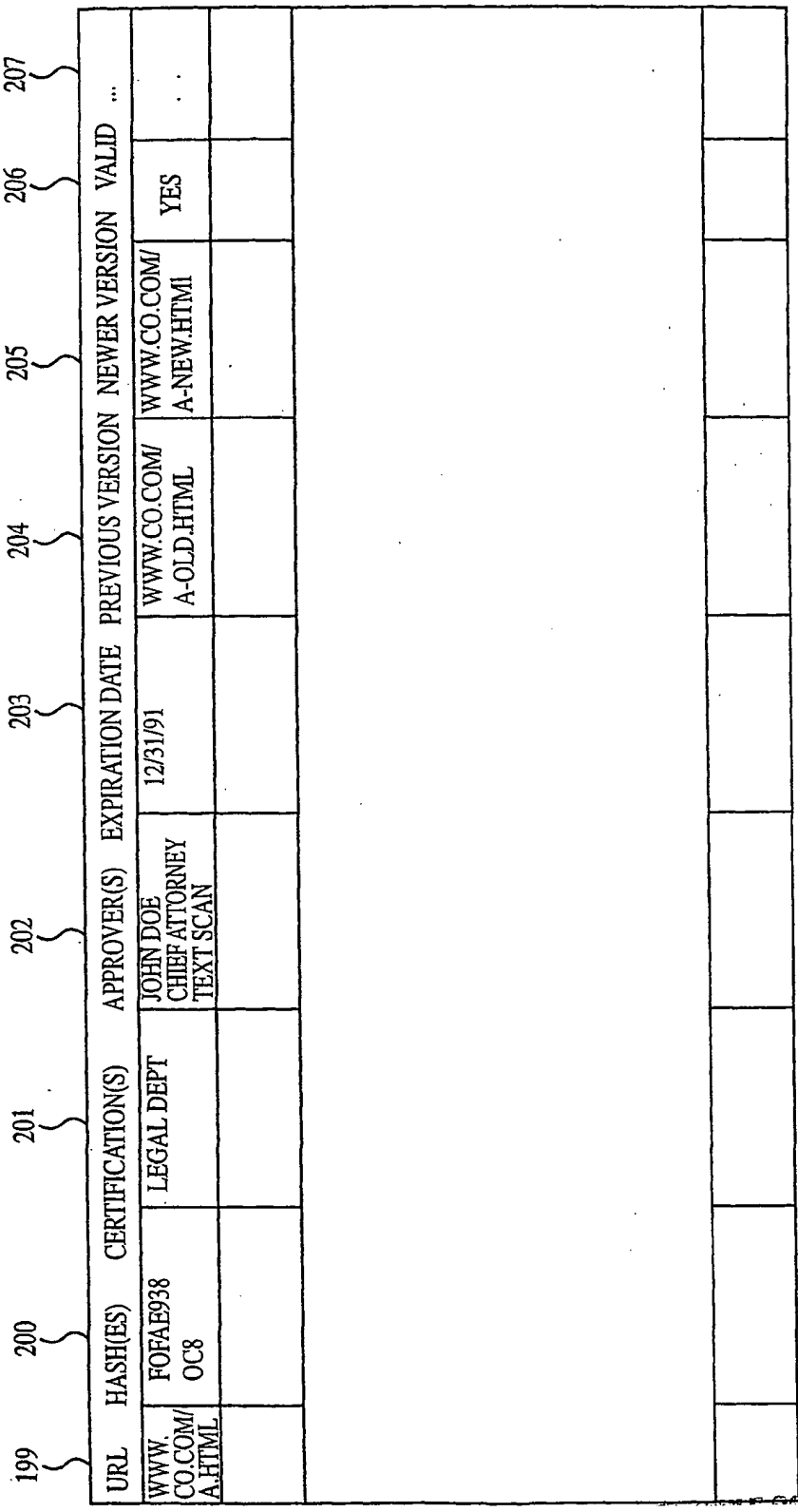


FIG. 10

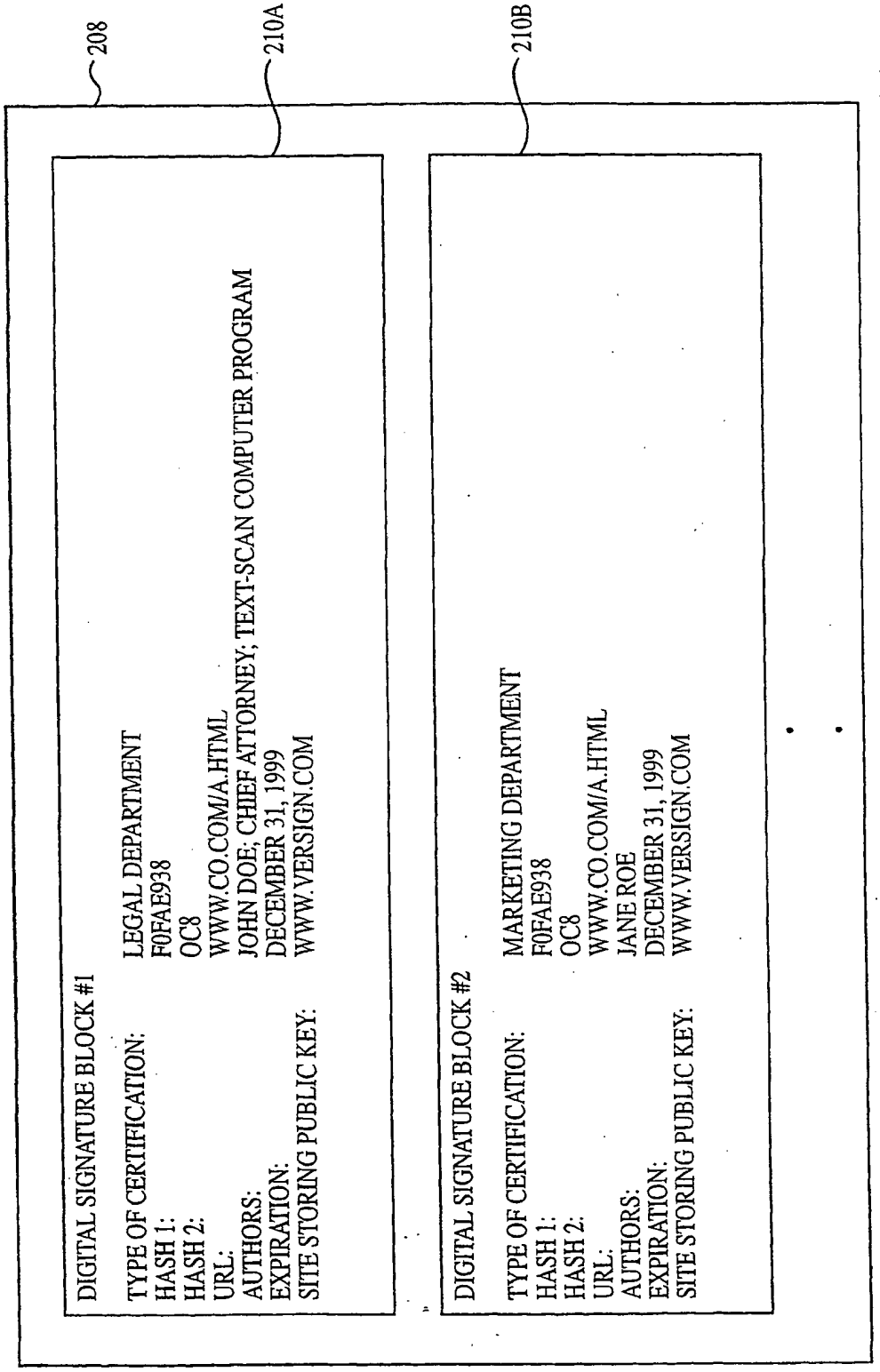


FIG. 11

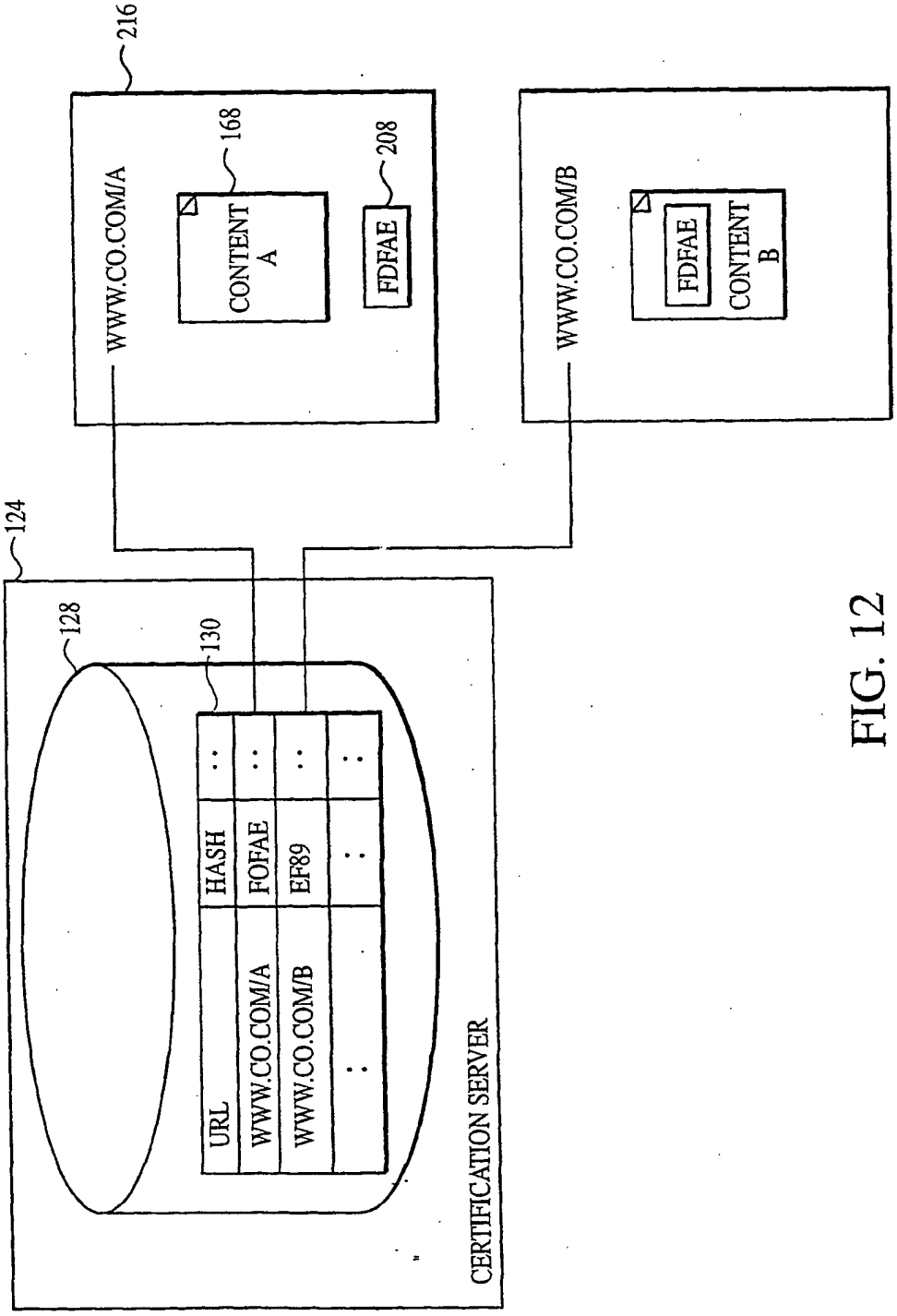


FIG. 12

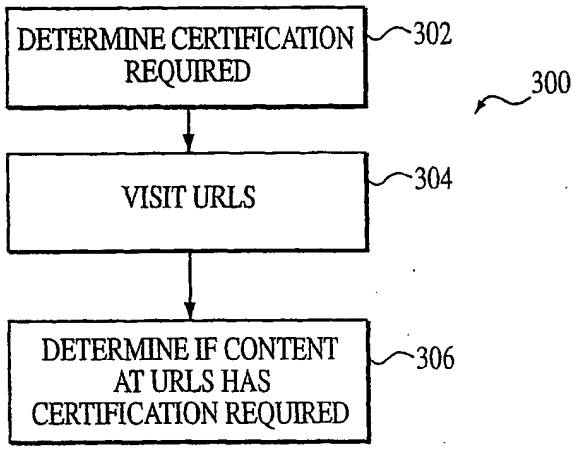


FIG. 13

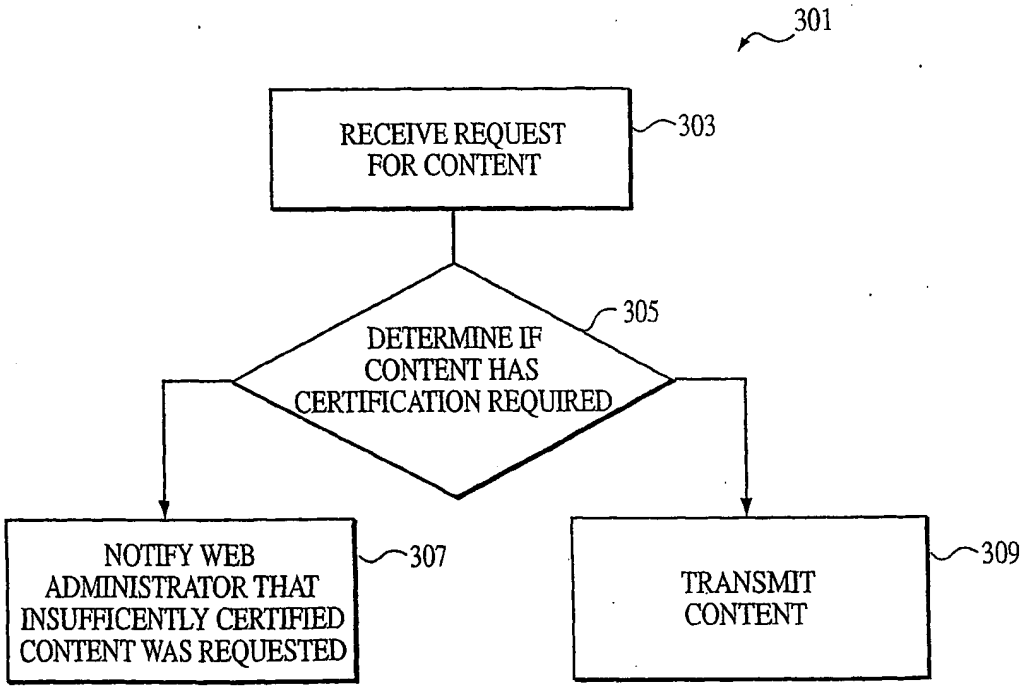


FIG. 14

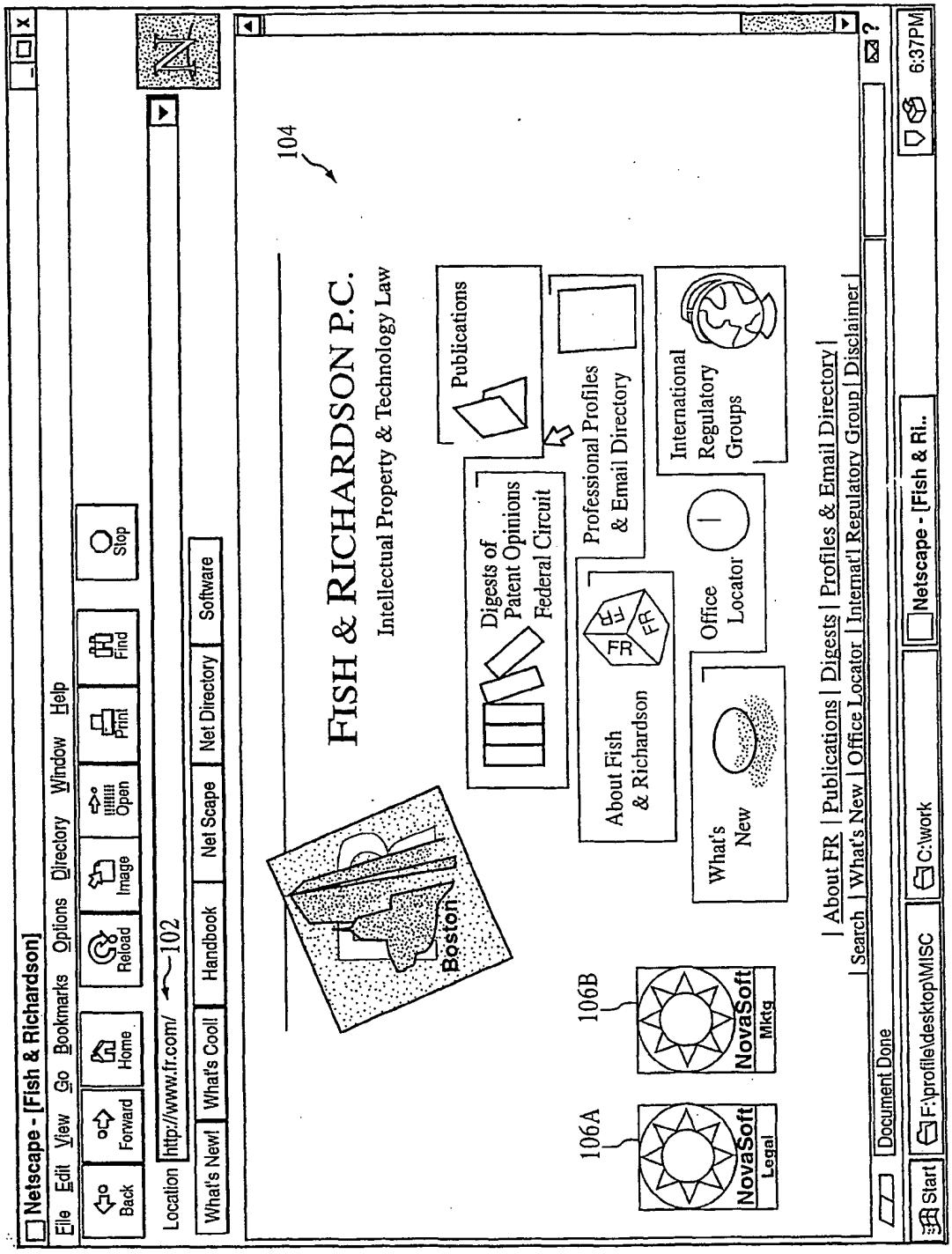


FIG. 15

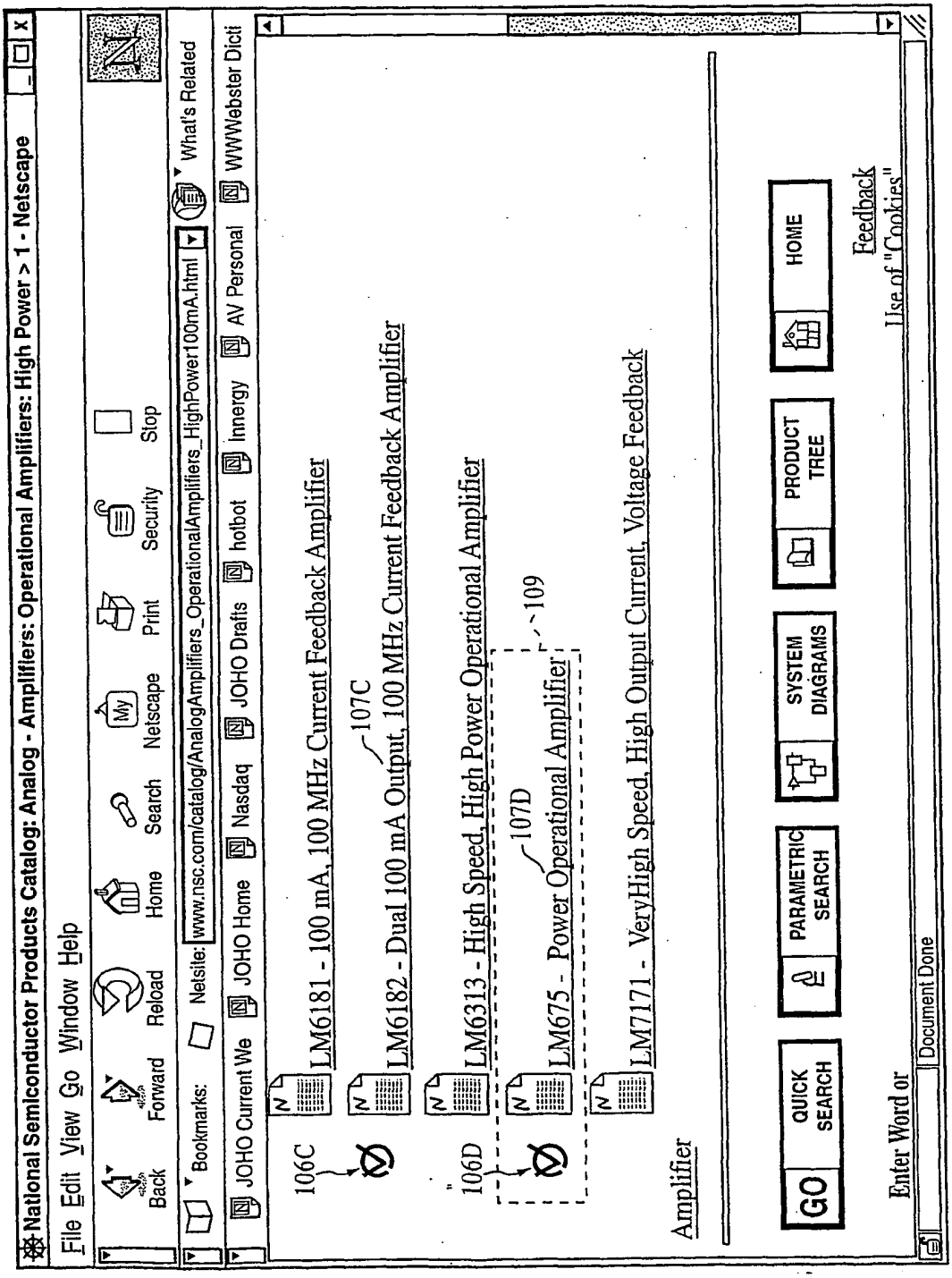


FIG. 16

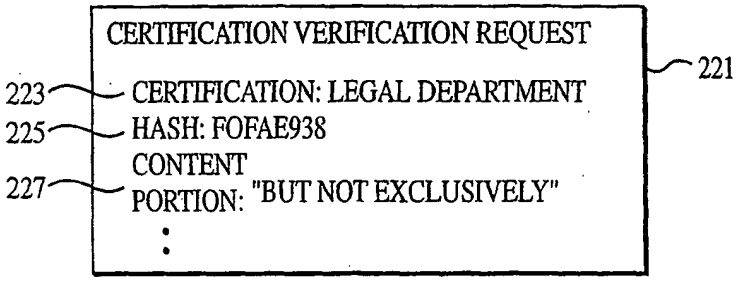


FIG. 17

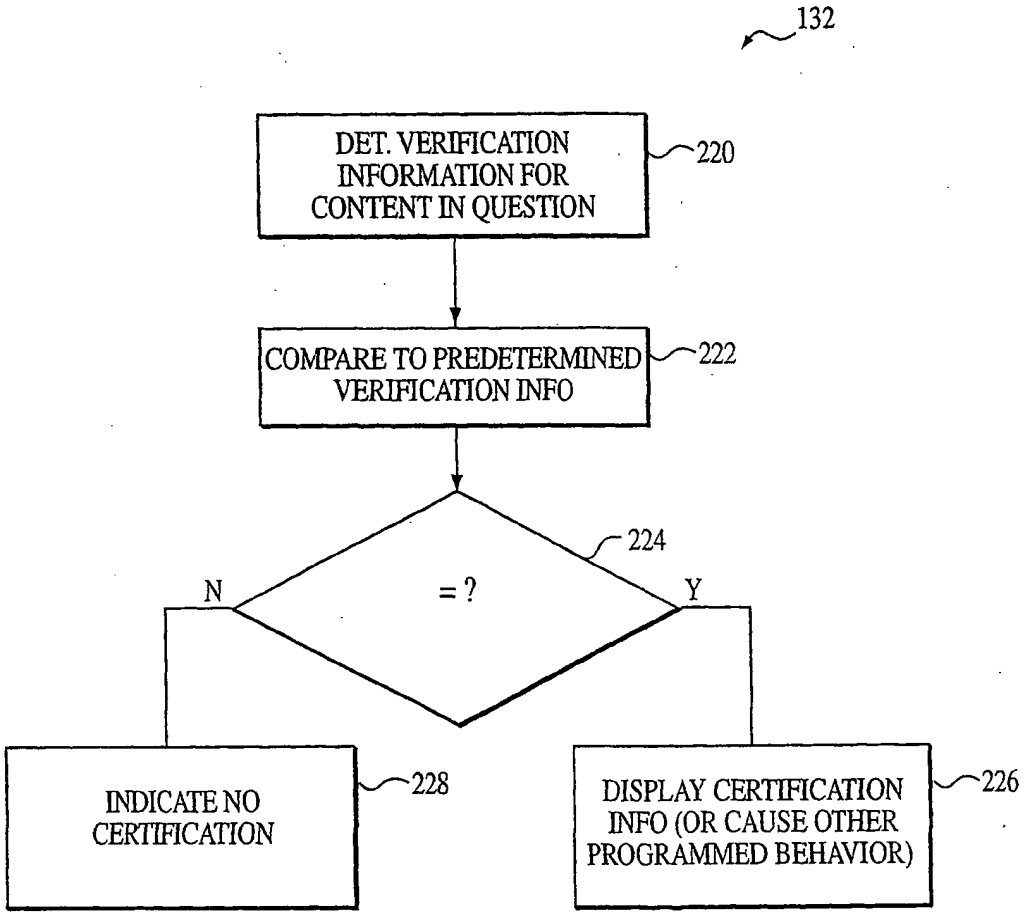


FIG. 18

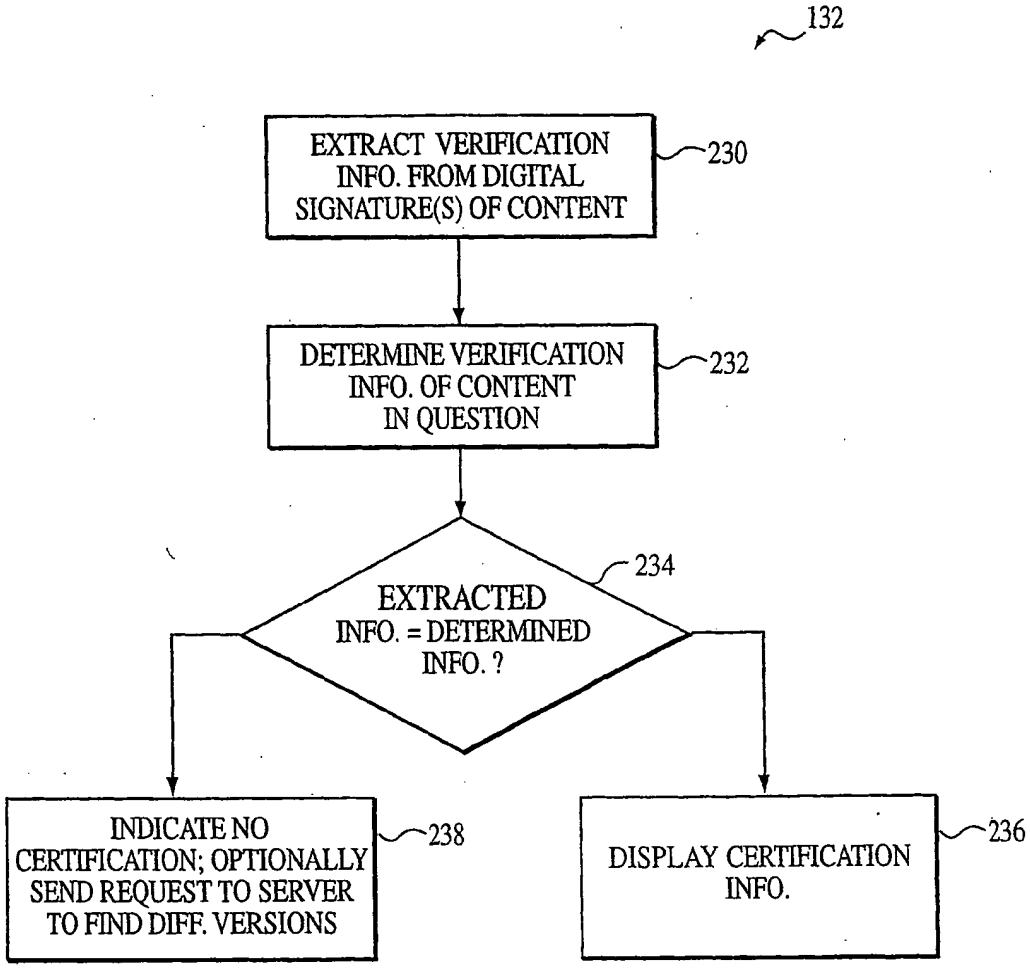


FIG. 19

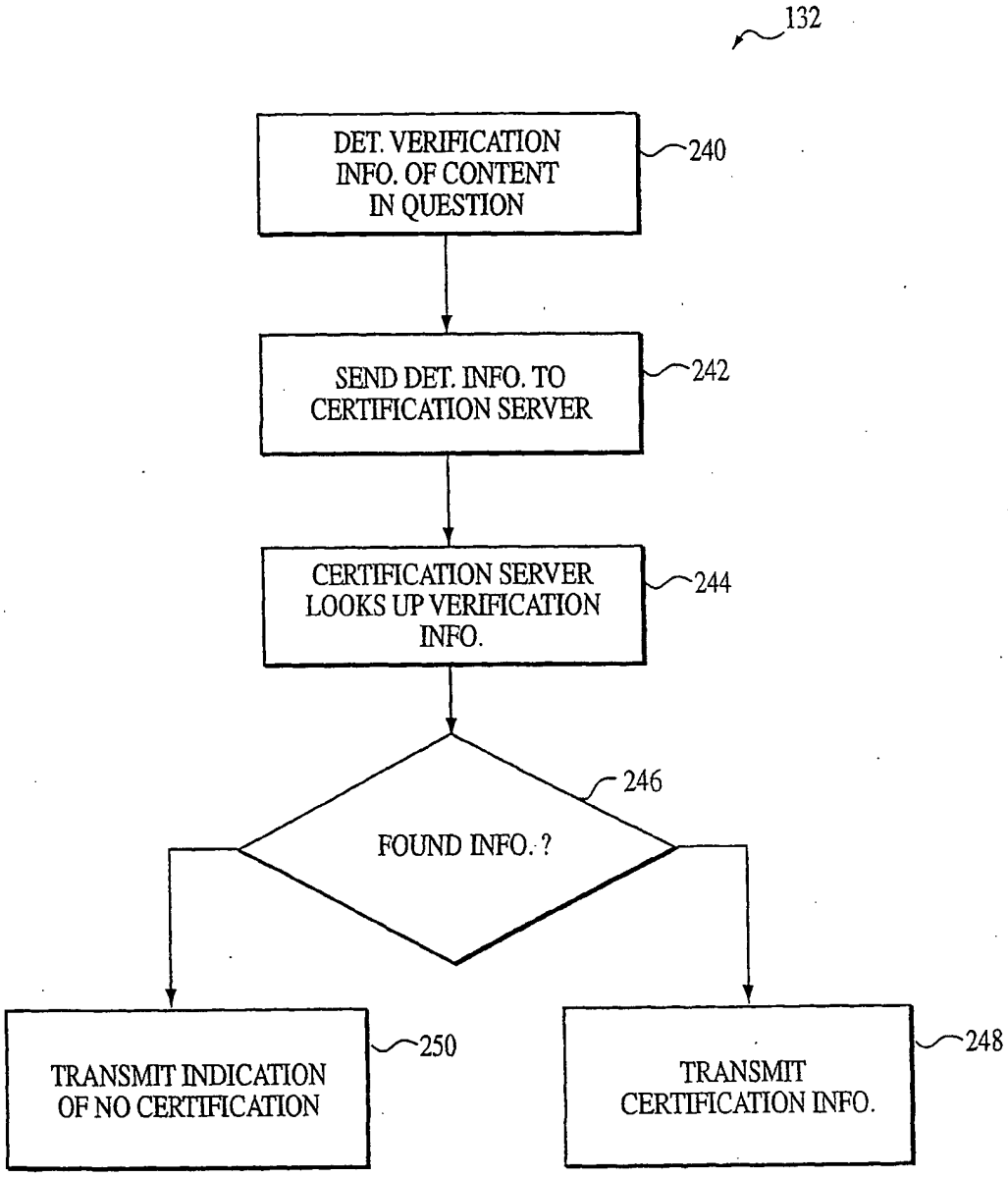


FIG. 20

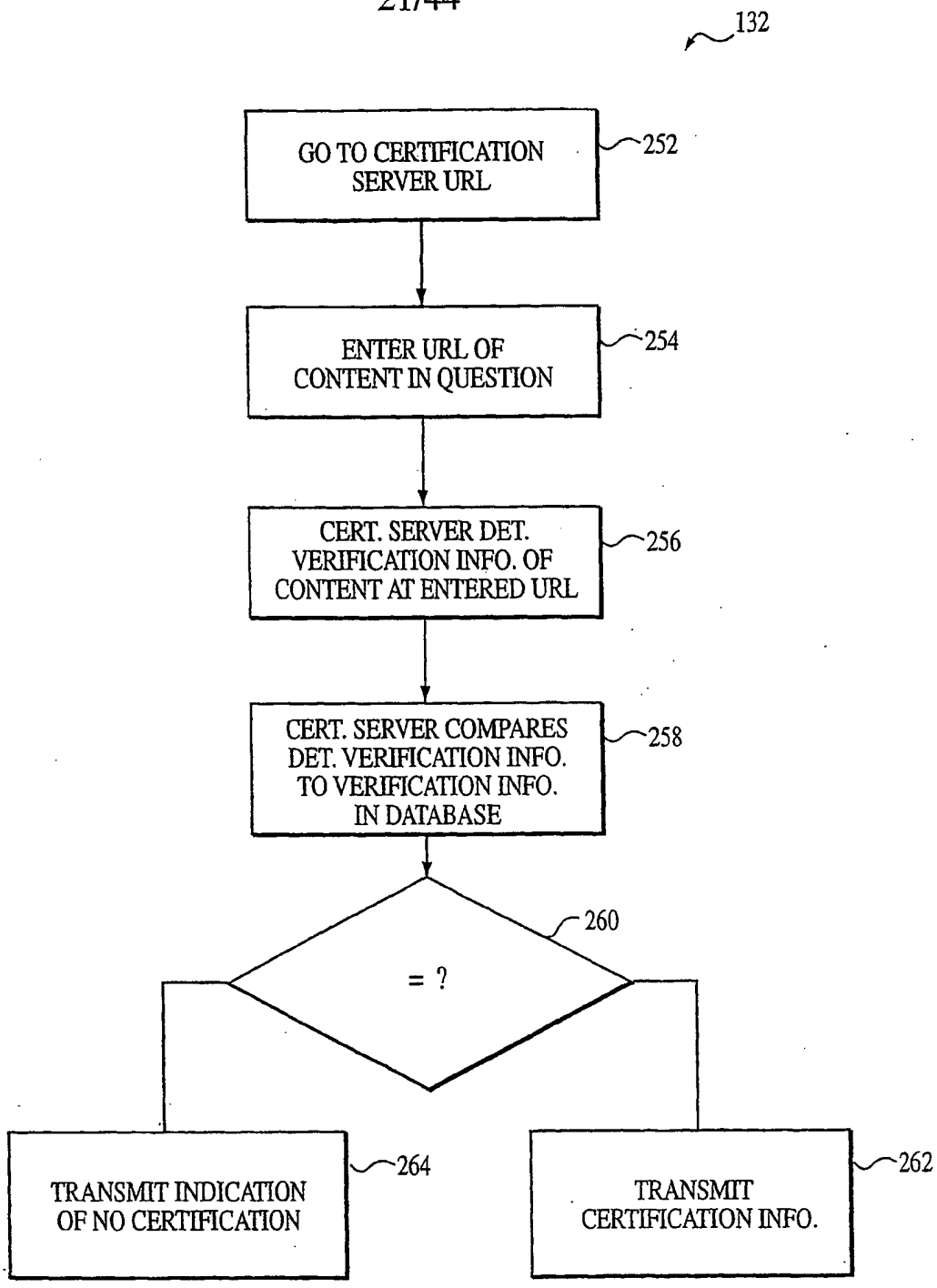


FIG. 21

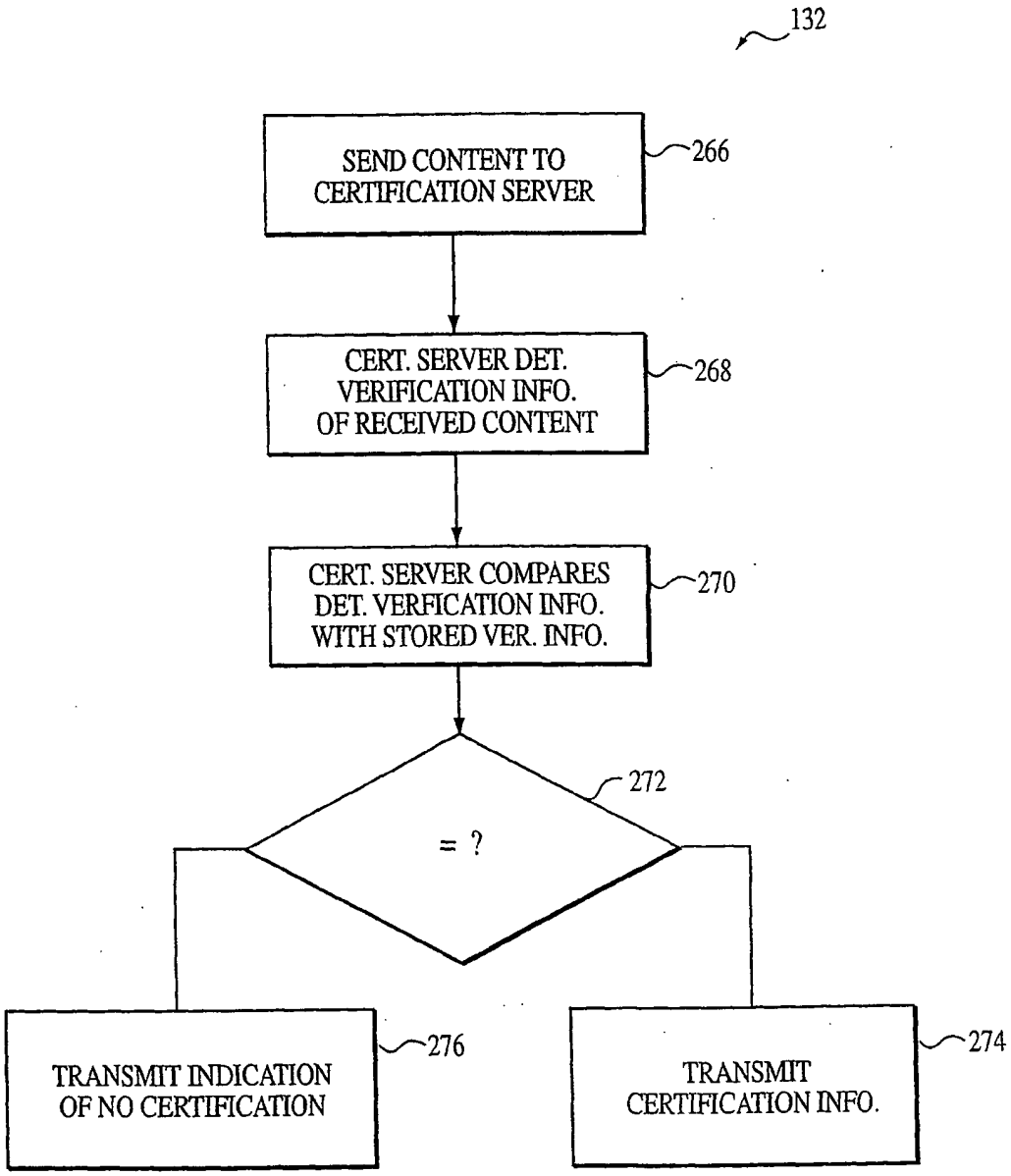


FIG. 22

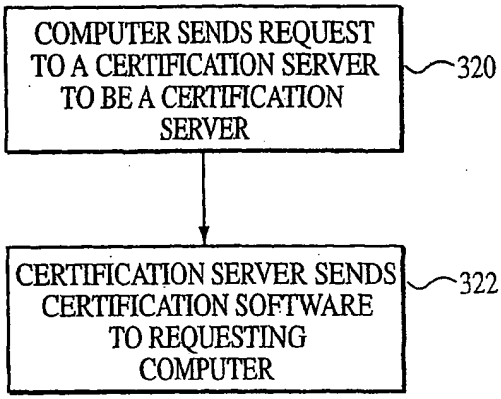


FIG. 23

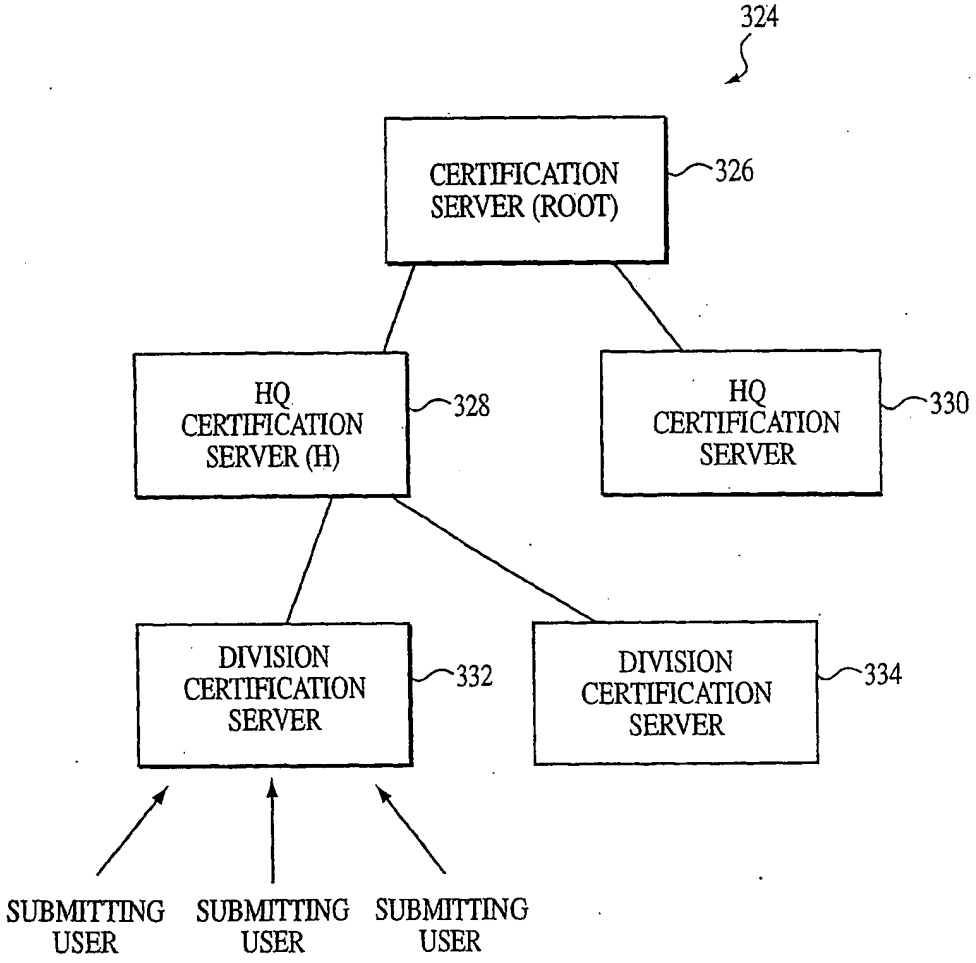


FIG. 24

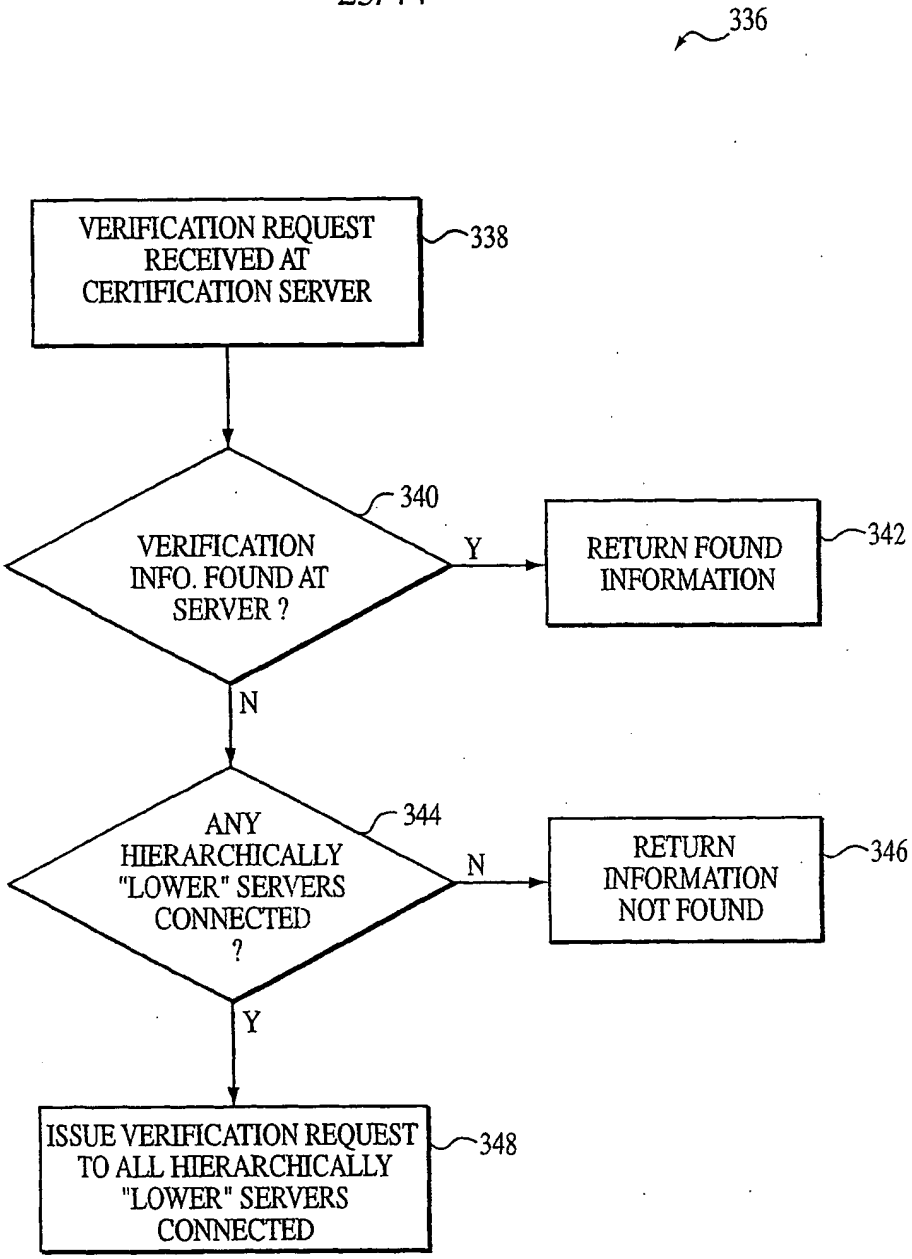


FIG. 25

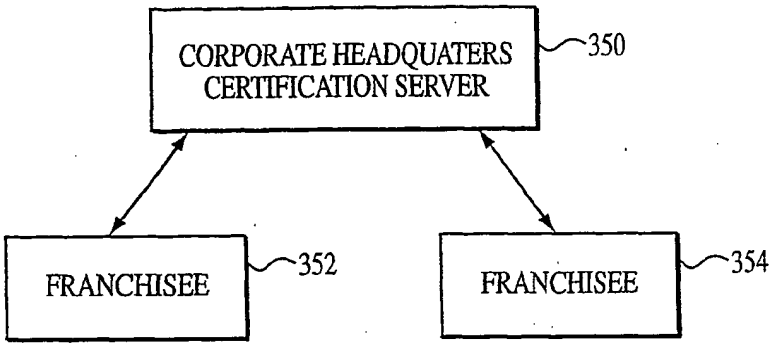


FIG. 26

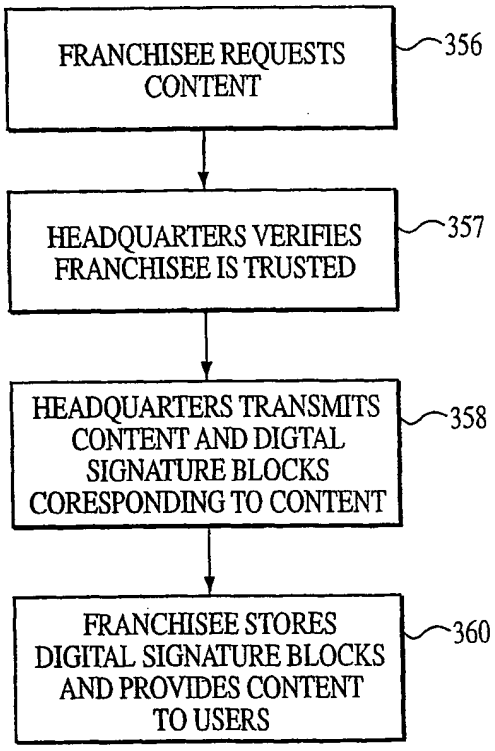


FIG. 27

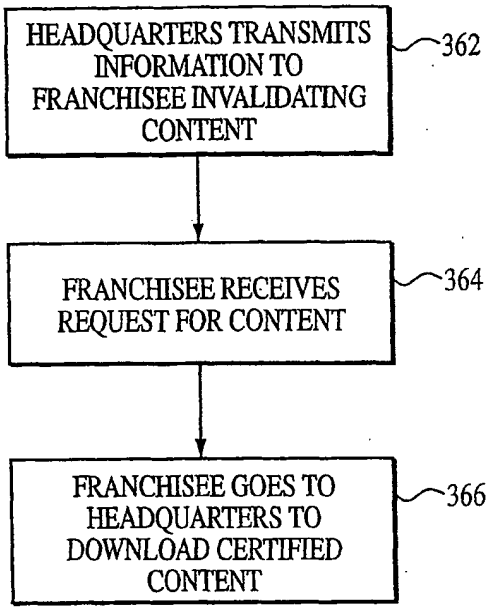


FIG. 28

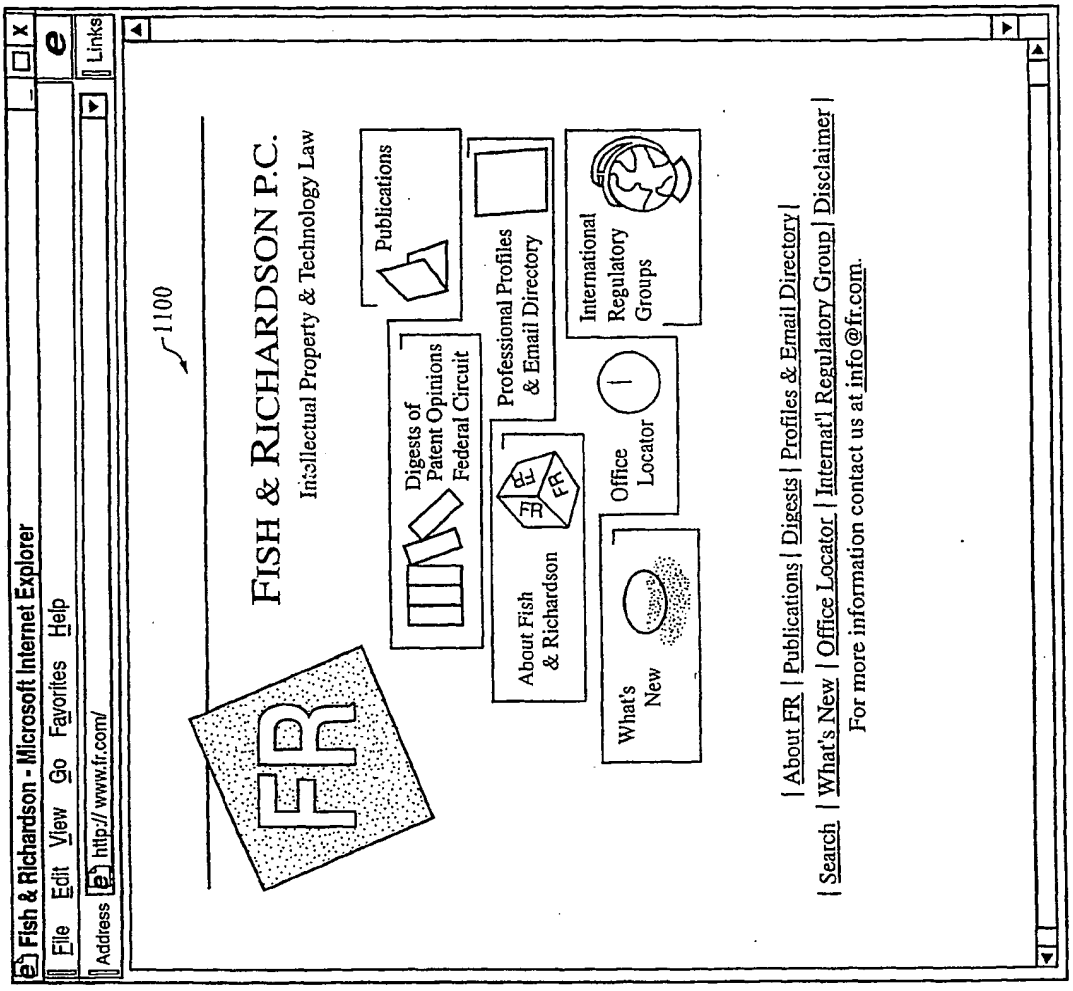


FIG. 29

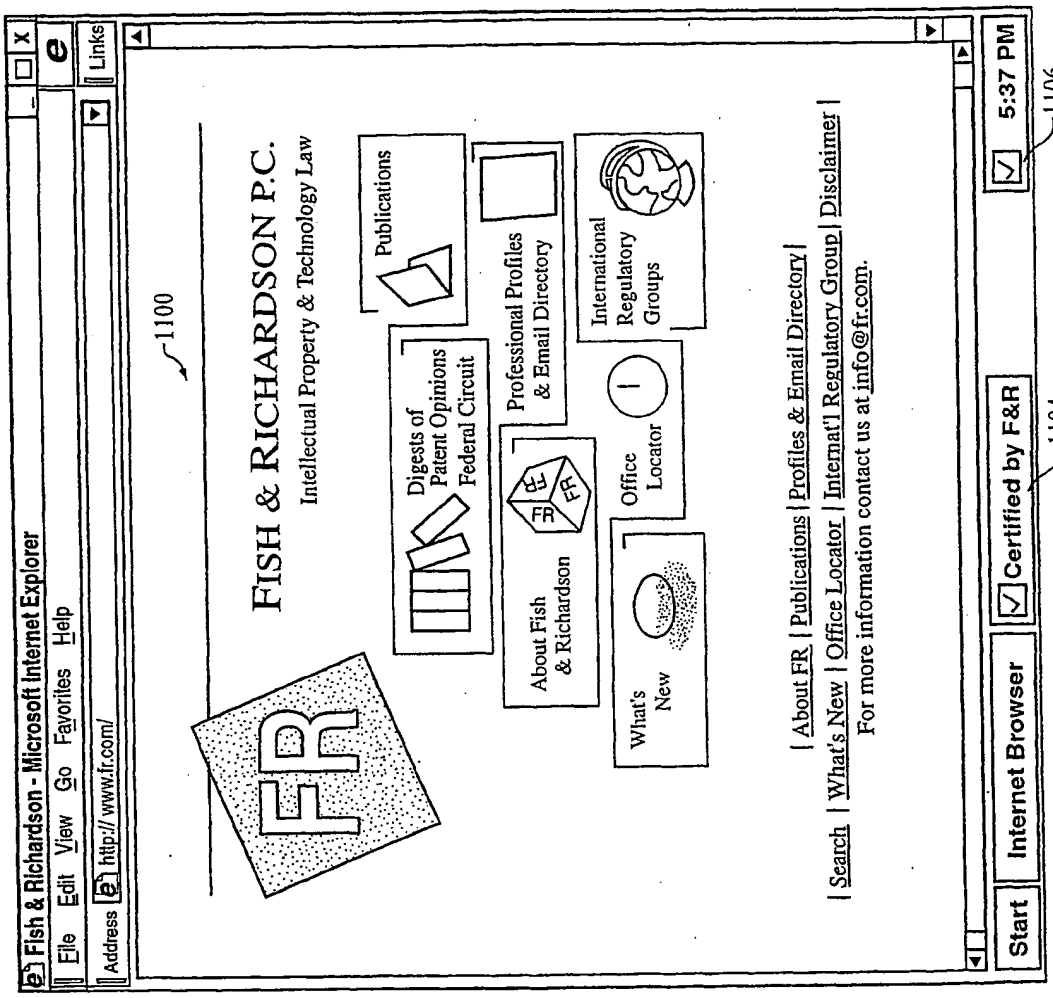


FIG. 30

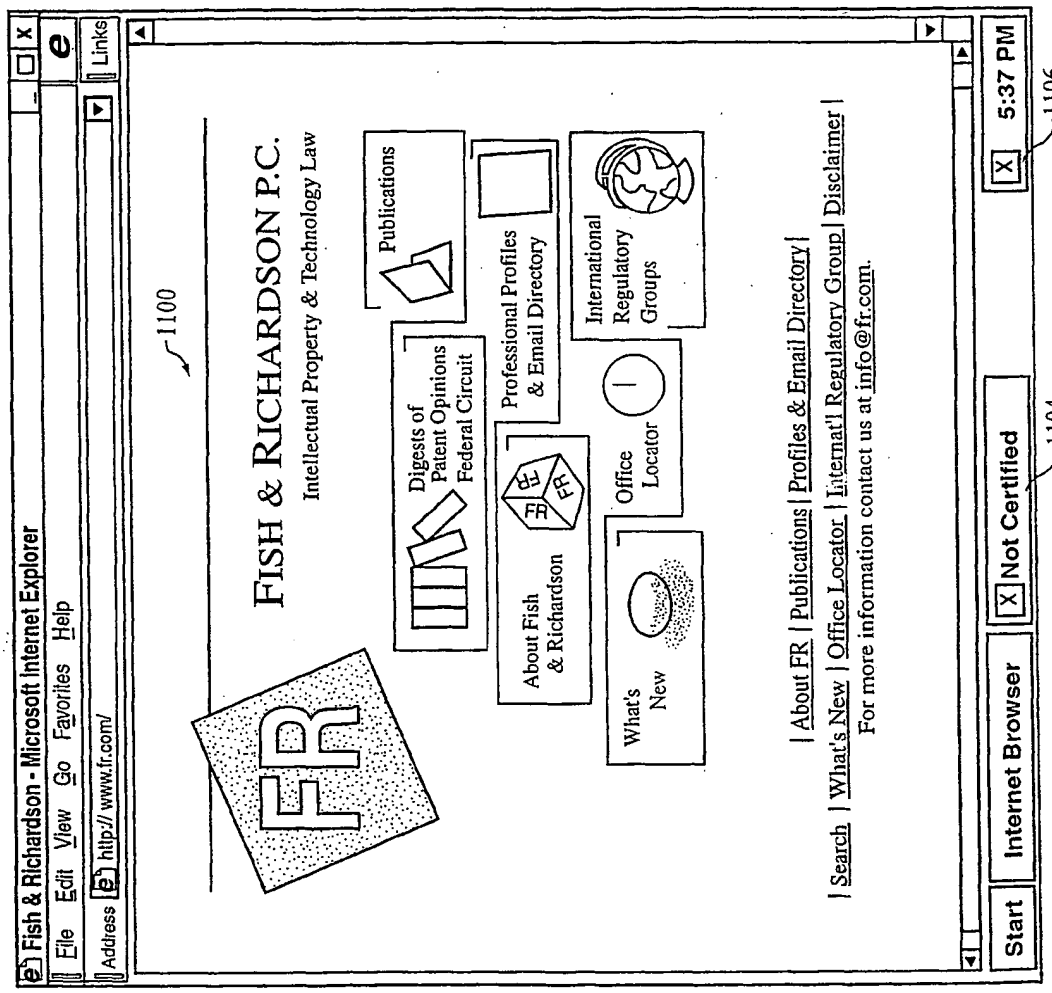


FIG. 31

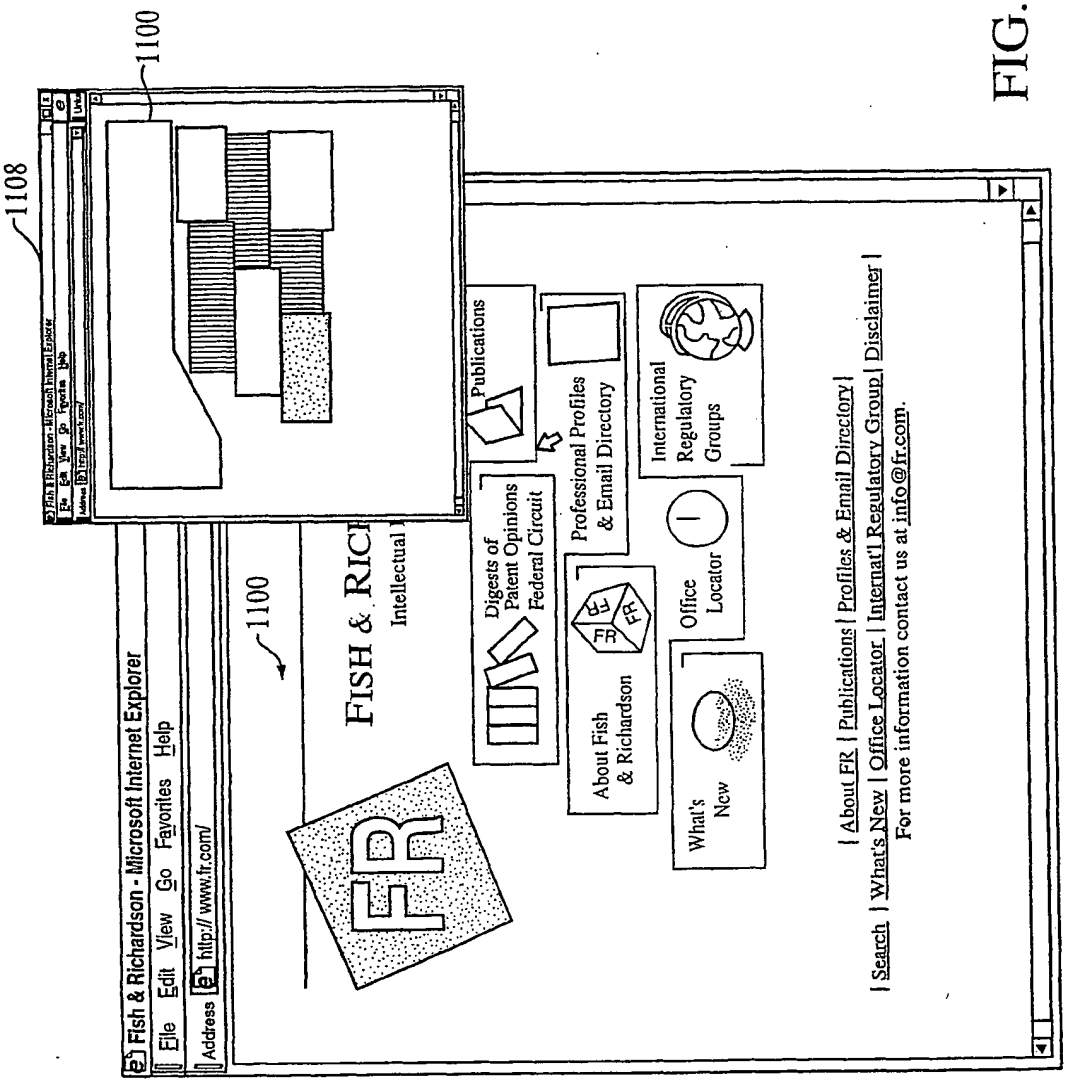


FIG. 32

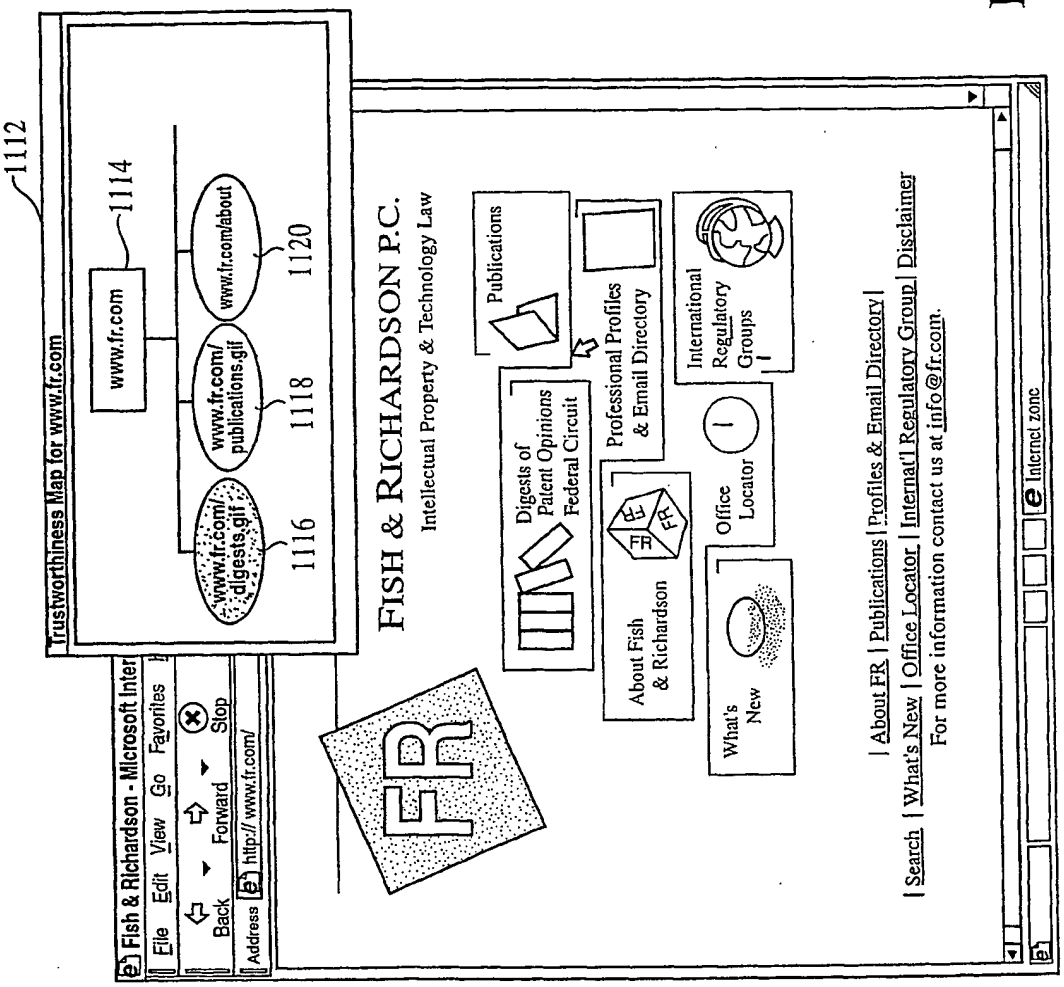


FIG. 33

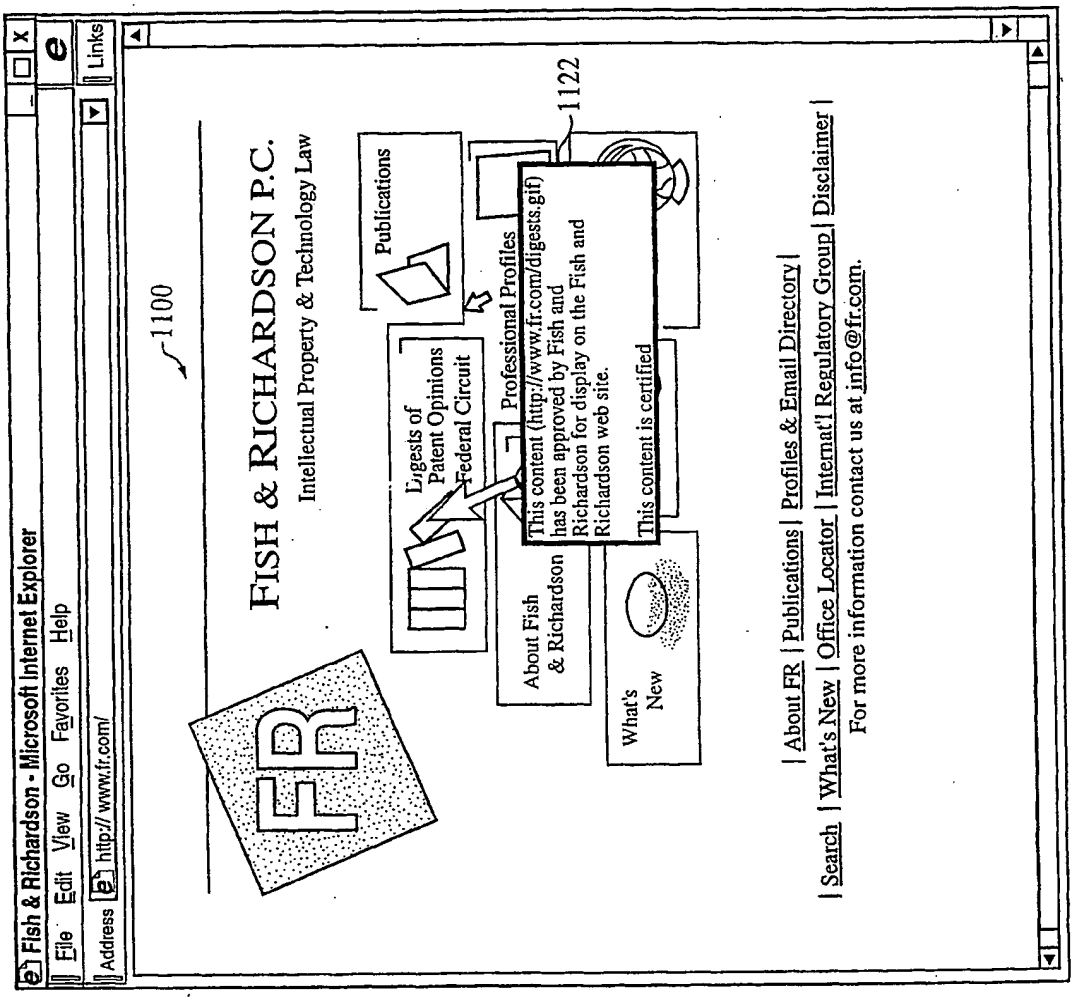


FIG. 34

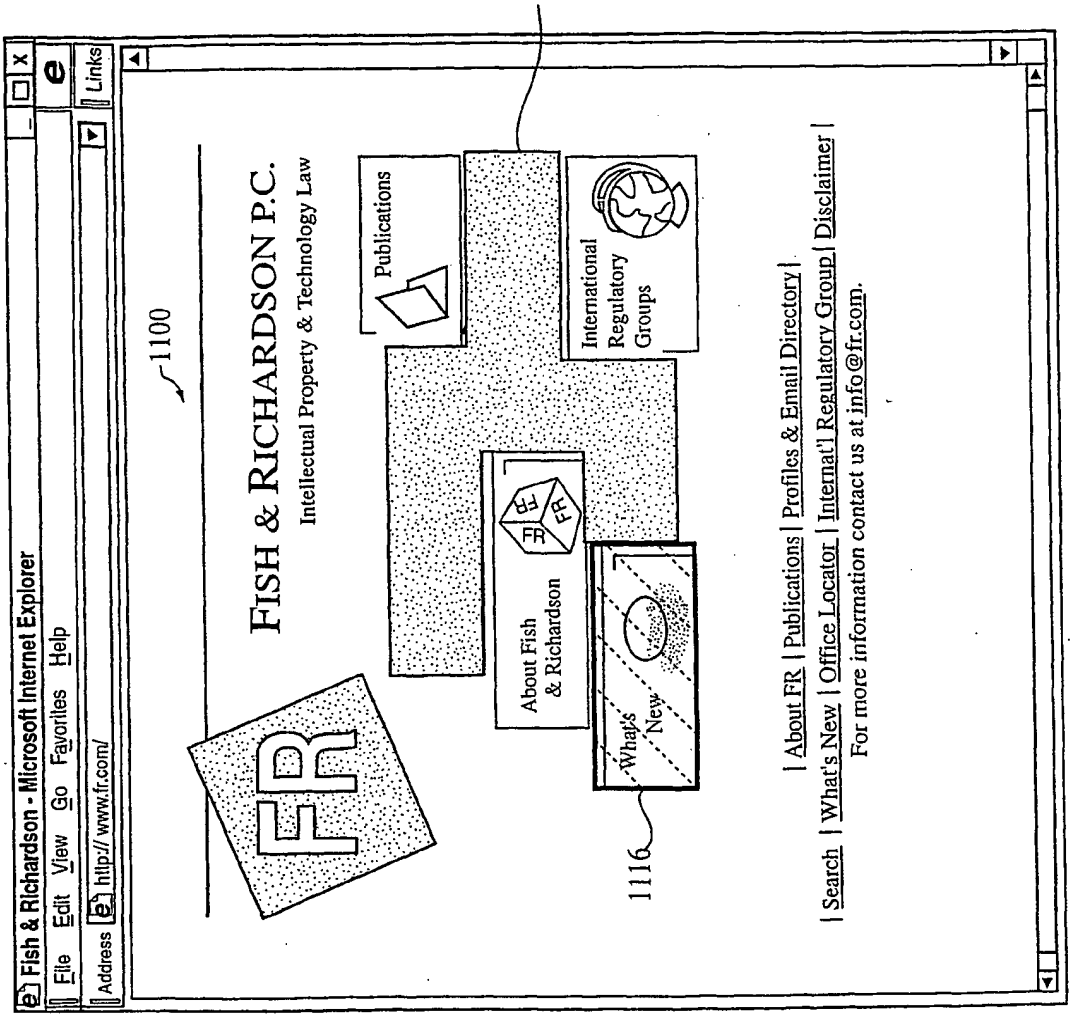


FIG. 35

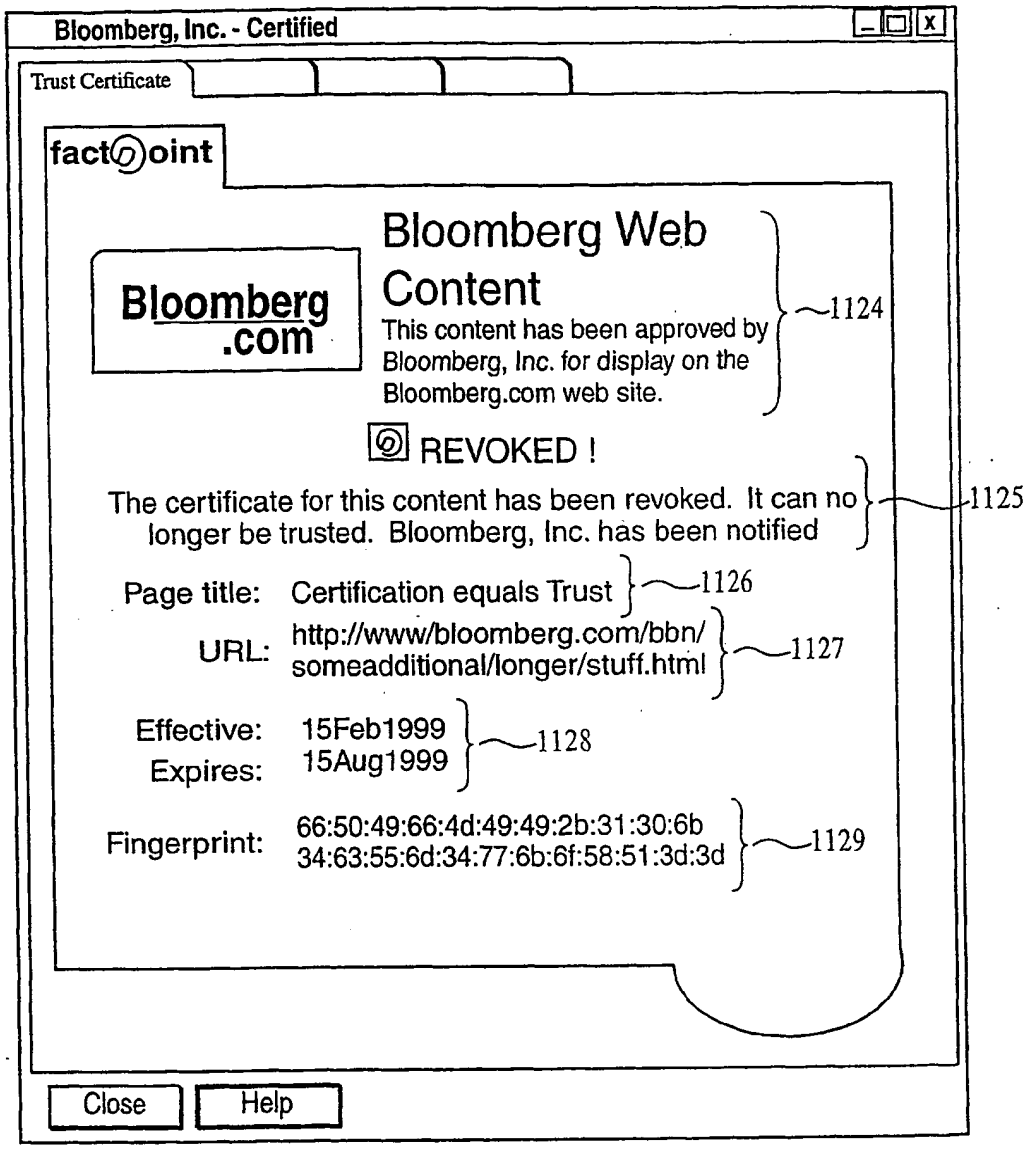


FIG. 36

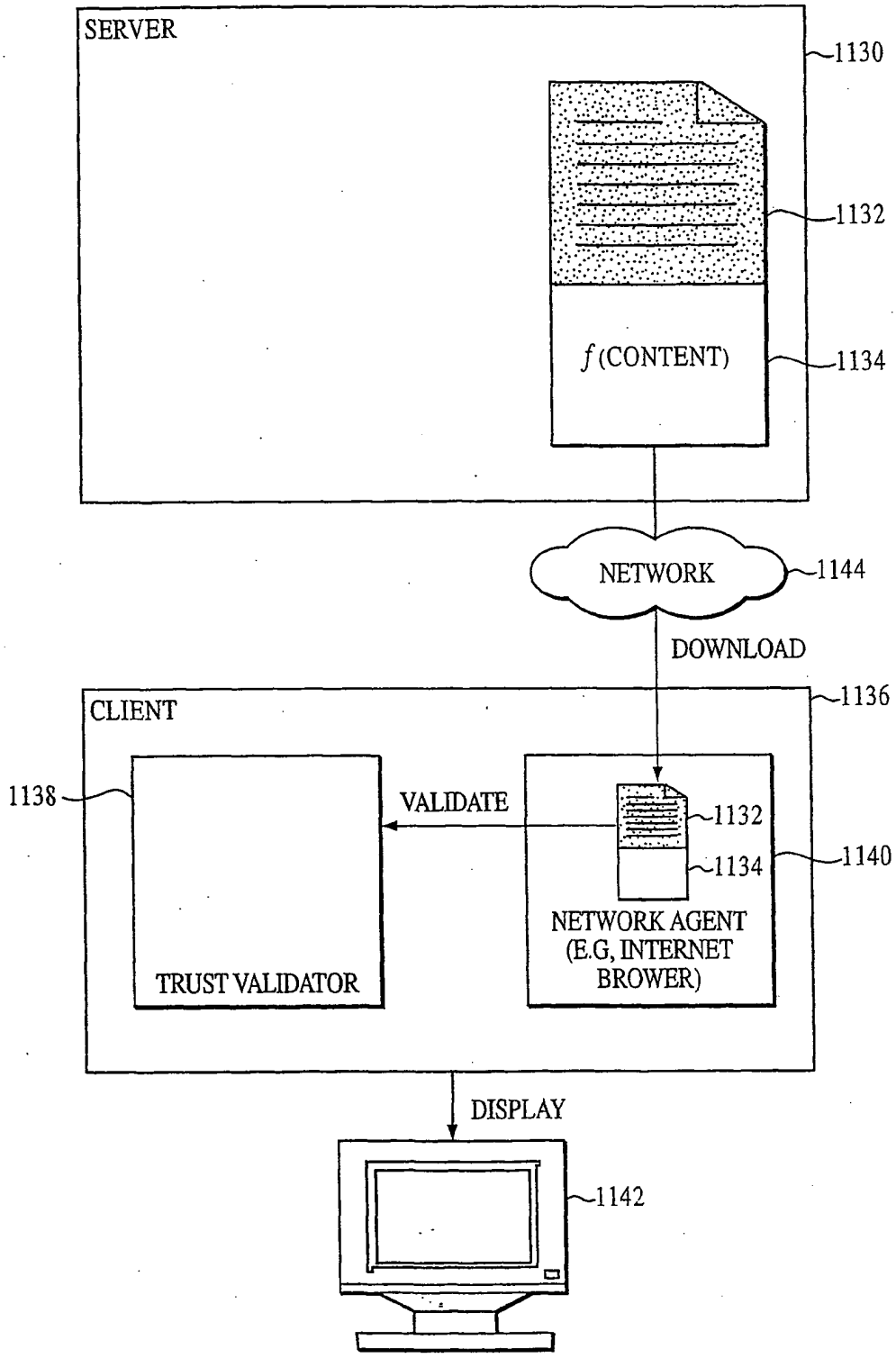


FIG. 37

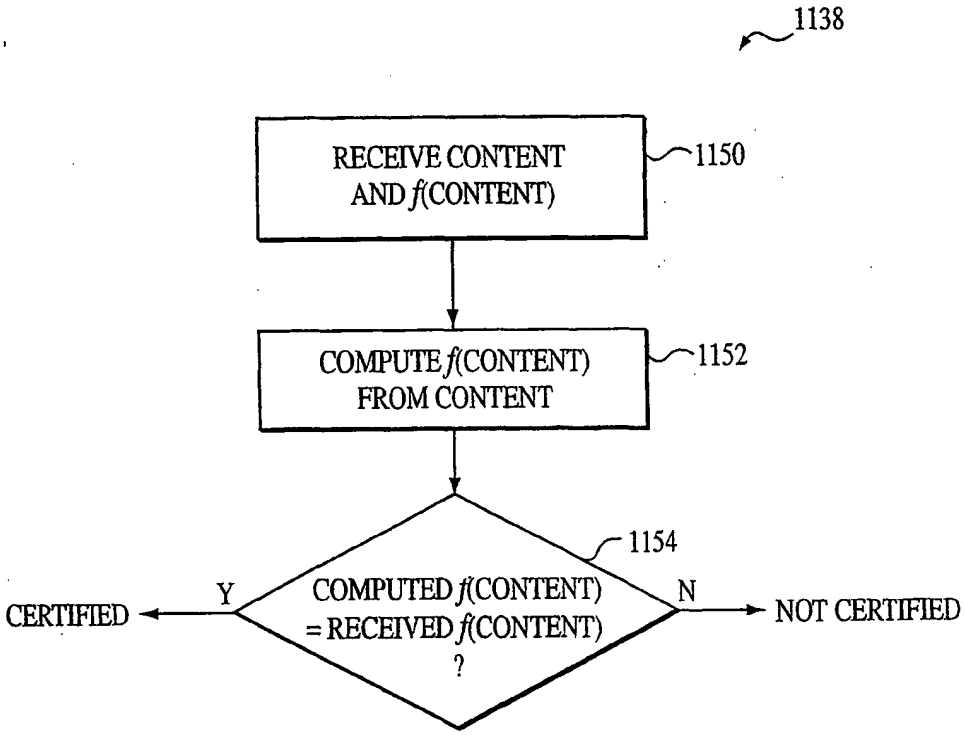


FIG. 38

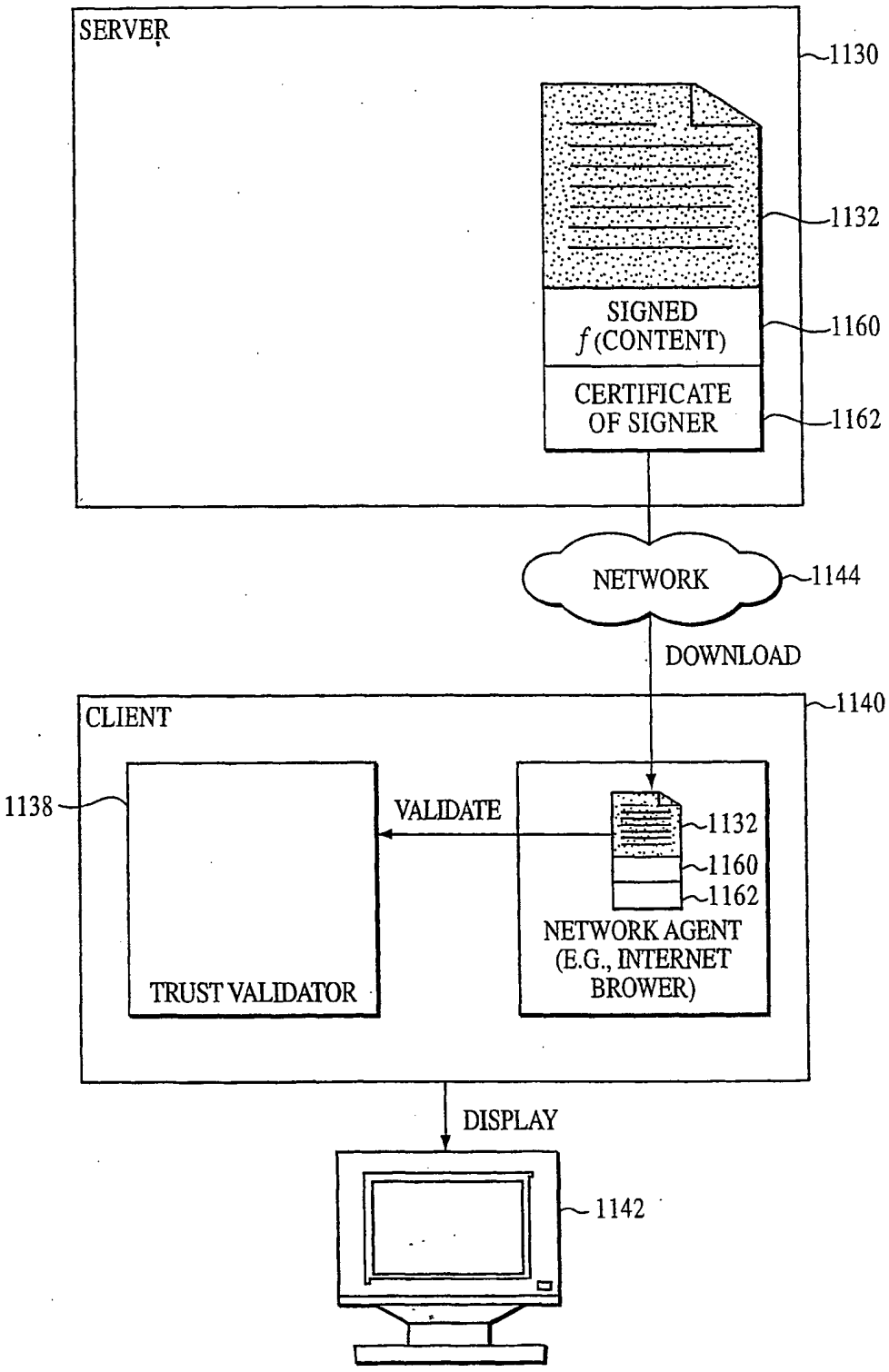


FIG. 39

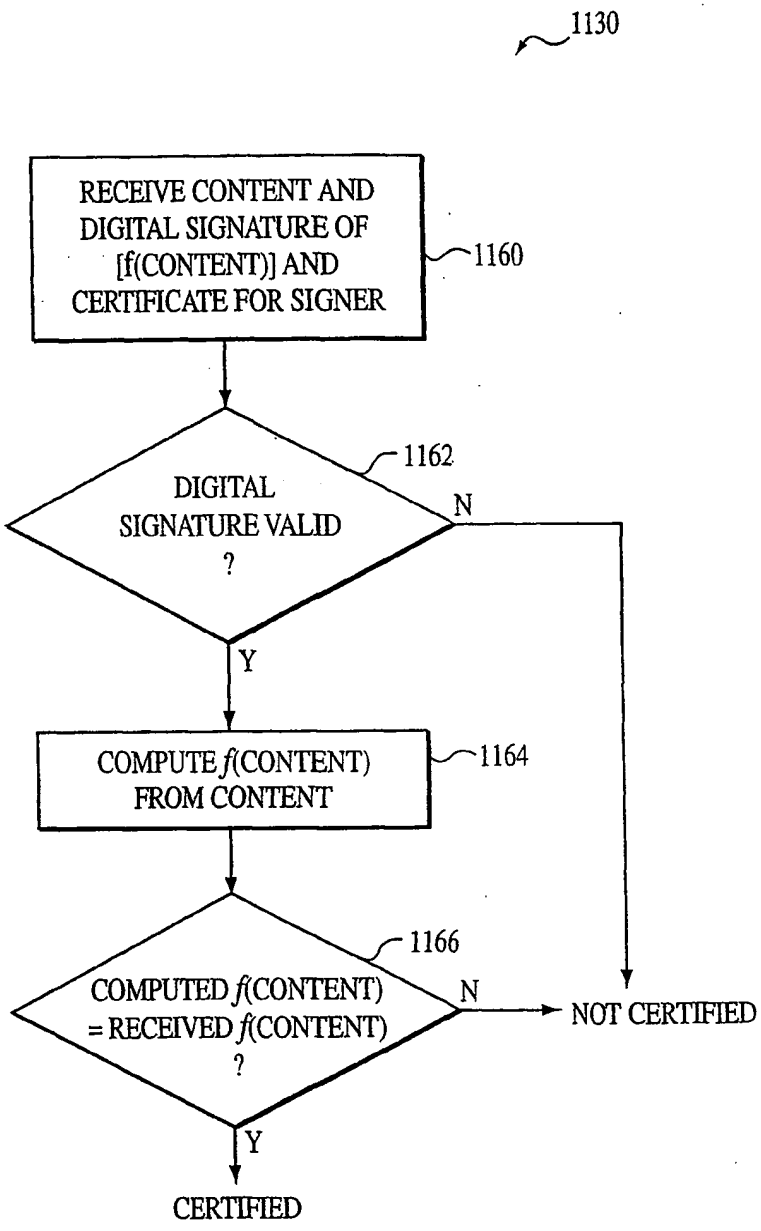


FIG. 40

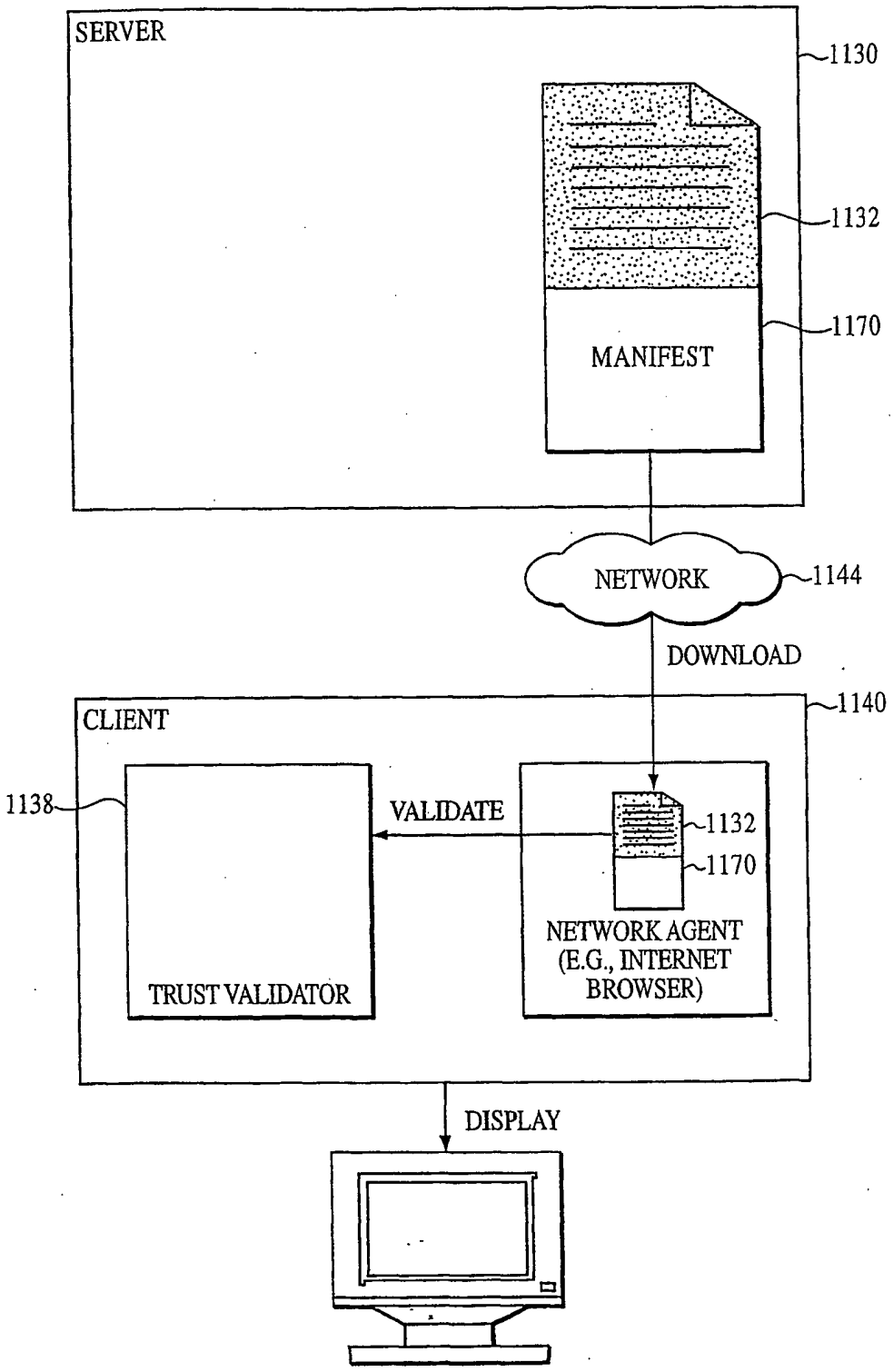


FIG. 41

1170

CONTENTS	f(CONTENT)
WWW.FR.COM	984EMF9
WWW.FE.COM/DIGEST.GIF	29482JD9
WWW.FR.COM/PUBLICATIONS.GIF	2930843F
WWW.FR.COM/ABOUT.GIF	23901233
•	
•	

FIG. 42

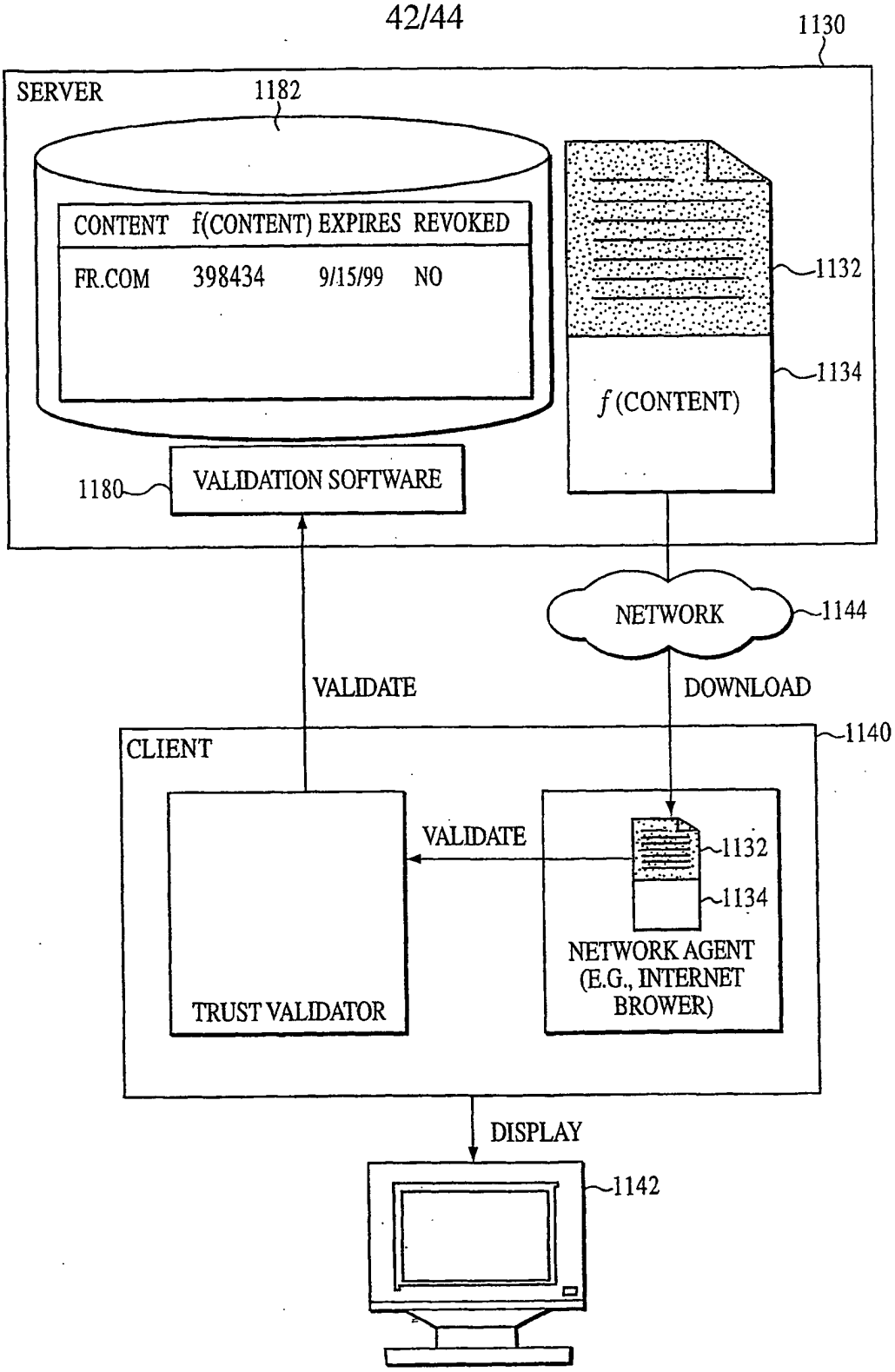


FIG. 43

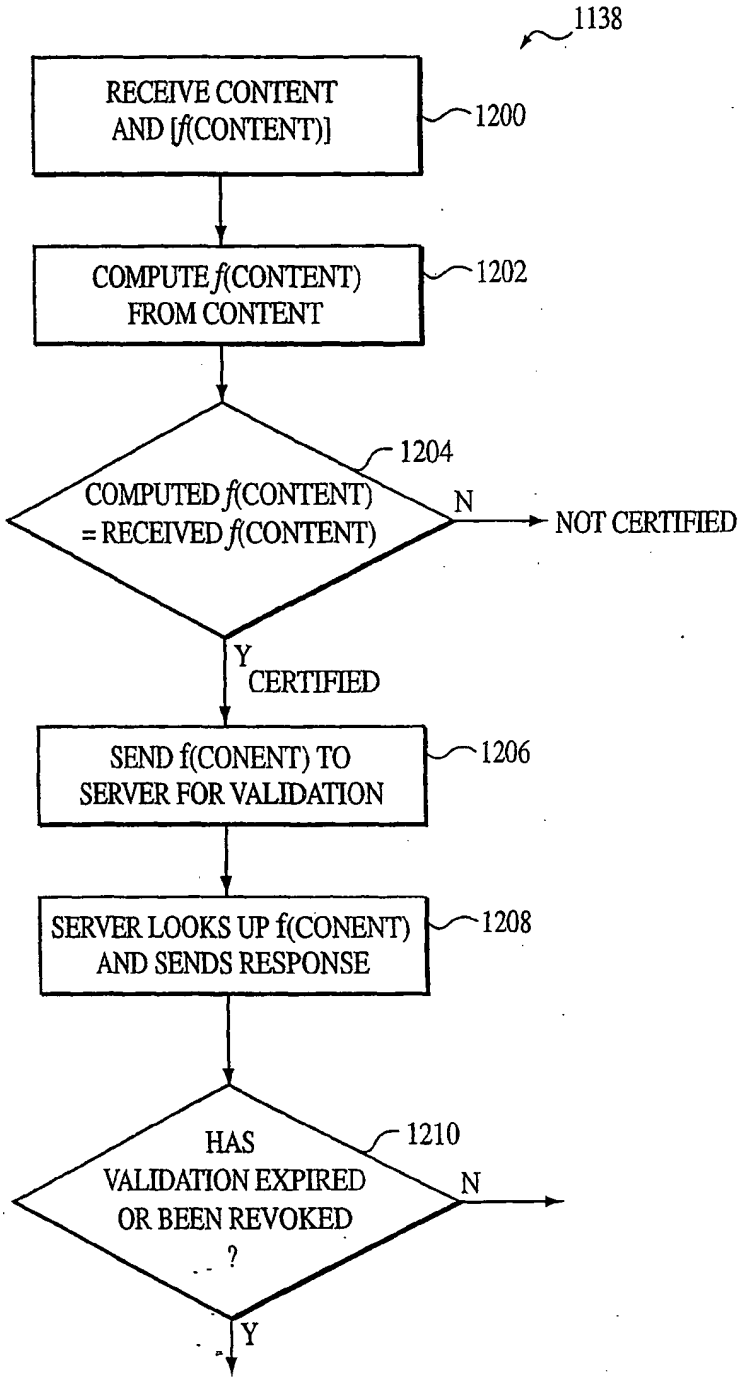


FIG. 44

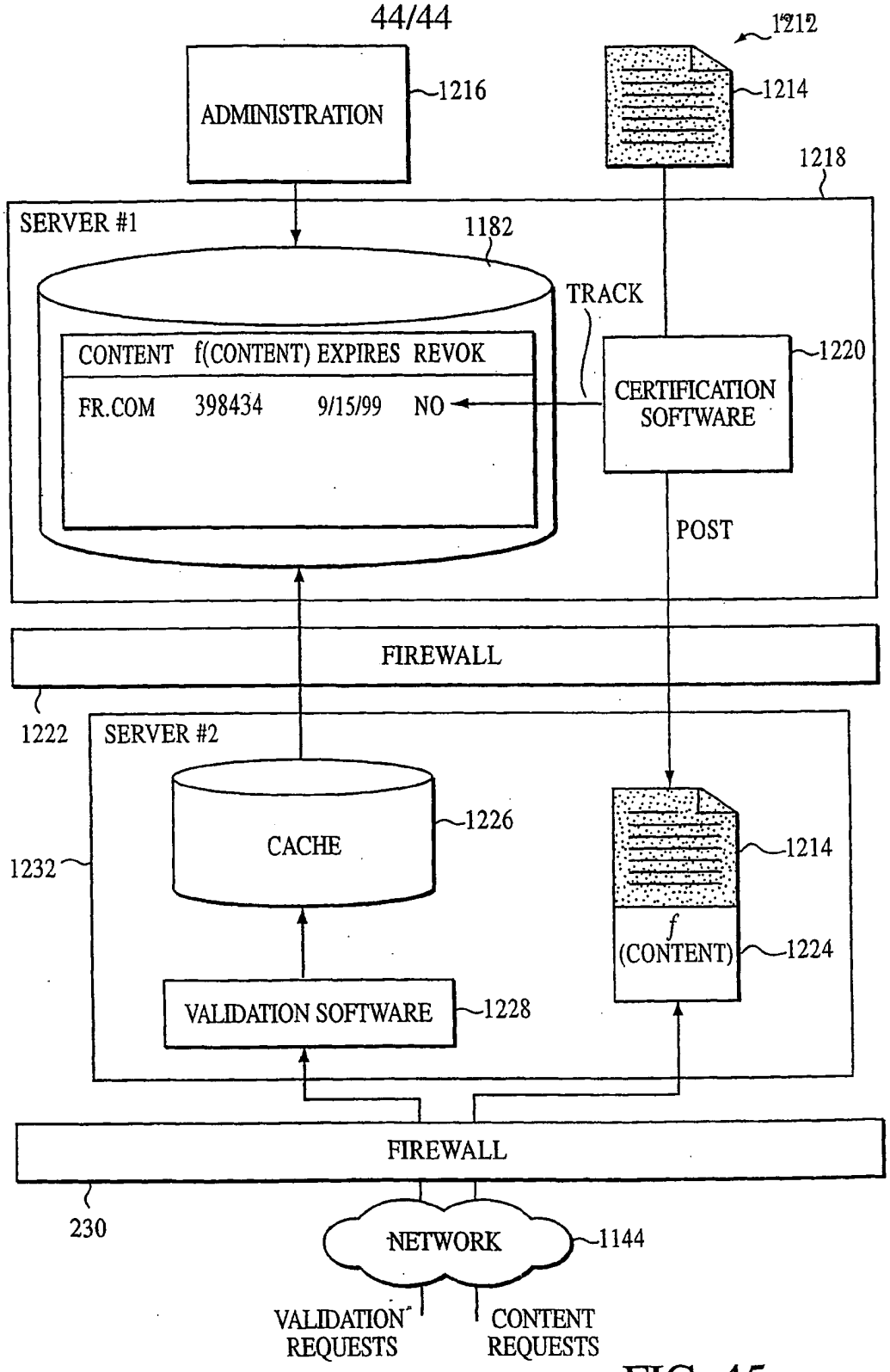


FIG. 45

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/03489

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) :G06F 13/00
US CL :709/200; 705/44; 713/201

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 709/200; 705/44; 713/201

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A,T	US 6,058,383 A (NARASIMHALU ET AL) 02 MAY 2000, ALL	1-42
A,T	US 6,026,166 A (lEBOURGEOIS) 15 FEBRUARY 2000, ALL	1-42
A,P	US 5,903,882 A (ASAY ET AL) 11 MAY 1999, ALL	1-42
A,P	US 6,018,724 A (ARENT) 25 JANUARY 2000, ALL	1-42

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search	Date of mailing of the international search report
27 JUNE 2000	19 JUL 2000
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer GLENTON BURGESS Telephone No. (703) 305-4792

Form PCT/ISA/210 (second sheet) (July 1998) ★